3PAR Recovery Manager 4.1.0 for Microsoft Exchange 2007 User's Guide

3PAR, Inc.
4209 Technology Drive
Fremont, CA 94538 USA

Part No. 320-200245 Rev A
September 2010

3PAR Confidential

Revision Notice
This is the first release of this manual. A complete revision history is provided at the end of this manual.

Changes
The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, 3PAR Inc. assumes no liability resulting from errors or omissions in this document or from the use of the information contained herein.
3PAR reserves the right to make changes in the product design without reservation and without notification to its users.

Updates to the Documentation at 3PAR Central
Any updates to this document, or other 3PAR technical documents, can be found by logging into 3PAR Central's Document Control System from 3PAR's Support page, at: http://www.3par.com/support/index.html.

3PAR Technical Support and Services
Contact your local service provider for technical support and services.

Sales and Ordering Information
For sales and ordering information, contact
3PAR Inc.
4209 Technology Drive
Fremont, CA 94538 USA
Telephone: 510-413-5999
Fax: 510-413-5699
Email: salesinfo@3PAR.com

Reader Comments and Suggestions
Please email your comments and suggestions about this document to: ReaderComments@3PAR.com

Copyright
Printed Material
Copyright © 2010 3PAR Inc. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of 3PAR Inc., 4209 Technology Drive, Fremont, CA 94538. By way of exception to the foregoing, the user may print one copy of electronic material for personal use only.

Trademarks
3PAR, InServ, InForm, InSpire and Serving Information are registered trademarks of 3PAR Inc.
Microsoft Windows, Microsoft Exchange 2003 and Microsoft Exchange 2007 are trademarks of Microsoft, Inc.
All other trademarks and registered trademarks are owned by their respective owners.

Table of Contents

1 Introduction

1.1 Audience 1.1

1.2 Related Documents 1.2

1.3 Organization 1.3

1.4 Typographical Conventions 1.4

1.5 Advisories 1.5

2 Overview of Recovery Manager

2.1 System Requirements 2.2

2.2 Features Supported 2.3

2.3 Features not Supported 2.4

2.4 What's New in Recovery Manger for Exchange 4.1.0 2.4

2.5 Microsoft Volume Shadow Copy Service 2.4

2.6 How VSS Works with Exchange 2.6

2.7 Supported VSS Components 2.7

2.8 Recovery Manager Requirements 2.7

2.9 Recovery Manager Layout 2.8

2.9.1 Centralized Backup Configuration 2.8

2.9.2 Single Host Backup Configuration 2.10

2.9.3 CCR Backup Configuration 2.10
2.9.4 The Server Relationship 2.12

3 Installation and Deinstallation

3.1 Upgrading to Recovery Manager for Exchange 3.2
3.1.1 Production Server 3.2
3.1.2 Backup Server 3.2
3.1.3 Installing Recovery Manager 3.3
3.2 Verifying the Installation 3.5
3.3 Understanding the Registry 3.5
3.4 Environment Variables 3.7
3.5 Deinstalling Recovery Manager 3.7

4 Configuring Recovery Manager

4.1 Configuring the Database 4.2
4.2 Configuring Recovery Manager's Installation Location 4.2
4.3 Configuring Recovery Manager's Search Path 4.2
4.4 Configuring the Host Computer and the 3PAR InServ Storage Server 4.2
4.5 Configuring Recovery Manager Communications 4.2
4.6 Configuring the Policy for an Exchange Server 4.3
4.7 Configuring Recovery Manager for CCR 4.4

5 Configuring NetBackup for Recovery Manager

5.1 Overview 5.1
5.2 Defining a NetBackup Policy 5.2

6 Using the Recovery Manager GUI

6.1 Overview of the Recovery Manager GUI 6.2
6.1.1 Menu Bar 6.3
6.1.2 Node Tree Pane 6.4
6.1.3 Informational Right Pane 6.4
6.1.4 Displaying Server Information 6.4

3PAR Confidential

6.1.5 Displaying Storage Group Information **6.4**

6.2 Starting the GUI **6.6**

6.3 Stopping the GUI **6.6**

6.4 Server Registration **6.6**

6.5 Setting Recovery Manager Policy Configuration **6.6**

6.6 Creating a Virtual Copy **6.7**

6.6.1 To Create a Virtual Copy of a Storage Group **6.8**

6.6.2 Create a Remote Virtual Copy **6.8**

6.6.3 LCR Virtual Copy **6.8**

6.6.4 CCR Virtual Copy **6.9**

6.7 Mounting a Virtual Copy **6.10**

6.8 Unmounting a Virtual Copy **6.11**

6.9 Refreshing Virtual Copy Information **6.11**

6.9.1 Refreshing all Virtual Copies **6.11**

6.9.2 Refreshing all Virtual Copies for a Specific Storage Group **6.11**

6.9.3 Refreshing a Specific Virtual Copy **6.11**

6.10 Backing up a Virtual Copy Using Symantec NetBackup **6.11**

6.10.1 Backup at the Storage Group Level **6.12**

6.10.2 Backup at the Storage Group Level for CCR **6.12**

6.11 Restoring from Virtual Copy Timestamp **6.14**

6.11.1 File Copy Restore **6.14**

6.11.2 Volume Restore **6.14**

6.12 Restoring a Virtual Copy Using Symantec NetBackup **6.15**

6.13 Removing a Virtual Copy **6.16**

6.14 Virtual Copy Status **6.17**

6.15 Event Messages **6.17**

6.16 Analyzing the Repository **6.17**

6.17 Validating a Virtual Copy **6.18**

3PAR Confidential

7 Using the Recovery Manager CLI

7.1 Recovery Manager for Exchange Command Line Interface (CLI) **7.2**

7.2 Recovery Manager Commands **7.3**

7.3 Running Recovery Manager as a Scheduled Job **7.35**

8 Rapid Backup and Recovery for Exchange

8.1 Key Microsoft Exchange File Types **8.2**

8.2 Backup **8.3**

8.3 Virtual Copies **8.3**

8.3.1 Advantages of Using Recovery Manager **8.3**

8.4 Recovery Procedures **8.4**

8.4.1 Point-In-Time Recovery **8.4**

8.4.2 Volume Promote Point-In-Time Recovery **8.6**

8.4.3 Point-Of-Failure Recovery **8.8**

8.4.4 Single Mailbox Recovery **8.9**

8.4.5 Using the Recovery Storage Group Feature **8.13**

8.5 Additional Documentation **8.17**

9 Remote Copy for Recovery Manager

9.1 Purpose of Remote Copy **9.1**

9.2 How It Works **9.2**

9.3 Setting Up the Remote Copy **9.3**

9.3.1 Setting Up Remote Copy Groups for Storage Groups **9.3**

9.4 Recovering a Storage Group from a Secondary Site **9.3**

9.5 Synchronous Long Distance Remote Copy Support **9.4**

A Server Virtualization Environments

A.1 VMWare and Egenera **A.1**

B Troubleshooting

B.1 Known Issues **B.1**

B.2 Known Microsoft Issues **B.1**

3PAR Confidential

B.3 Troubleshooting B.2

C Event Messages

C.1 Description of Events C.11

Index

RH Revision History

3PAR Confidential

3PAR Confidential

1 Introduction

In this chapter

1.1 Audience 1.1

1.2 Related Documents 1.2

1.3 Organization 1.3

1.4 Typographical Conventions 1.4

1.5 Advisories 1.5

This guide provides the information you need to install, deinstall and use 3PAR Recovery Manager 4.1.0 for Microsoft Exchange 2007 with the Microsoft Windows 2008 Operating System.

1.1 Audience

This guide is designed for System Administrators and Microsoft Exchange Administrators who are responsible for backing up Microsoft Exchange mailbox or public store databases and who understand Microsoft Exchange 2007.

1.2 Related Documents

The following documents also provide information related to the InServ Storage Server:

For information about…	Read the…
Using the InForm command line interface (CLI) to configure and manage the InServ Storage Server	*3PAR InForm OS CLI Administrator's Manual*
Using the InForm Management Console's user interface to configure and manage the InServ Storage Server	3PAR InForm OS Management Console Online Help
Using the InForm Command Line Interface (CLI) for remote clients to install and configure Recovery Manager	*3PAR InForm OS Command Line Interface Reference*.
Identifying InServ Storage Server components and fixing problems	3PAR *InForm OS Messages and Operator's Guide*
Understanding the InServ Storage Server and its features	*3PAR InForm OS Concepts Guide*
Implementing shadow copies using 3PAR VSS Provider for Microsoft Windows	3PAR VSS Provider for Microsoft Windows User Guide

1.3 Organization

This guide is organized as follows:

- This chapter provides an overview of this guide, including intended audience, related documentation, typographical conventions, and advisories.
- Chapter 2, *Overview of Recovery Manager*, provides an overview of virtual copies and how Recovery Manager interacts with Microsoft Exchange.
- Chapter 3, *Installation and Deinstallation*, describes how to install, verify, and deinstall Recovery Manager.
- Chapter 4, *Configuring Recovery Manager*, contains instructions for configuring the database and Recovery Manager for Microsoft Exchange.
- Chapter 5, *Configuring NetBackup for Recovery Manager*, contains instructions for configuring Symantec NetBackup for use with Recovery Manager for Microsoft Exchange.
- Chapter 6, *Using the Recovery Manager GUI*, describes procedures for working with Recovery Manager through the GUI (Graphical User Interface).
- Chapter 7, *Using the Recovery Manager CLI*, describes procedures for working with Recovery Manager through the CLI (Command Line Interface).
- Chapter 8, *Rapid Backup and Recovery for Exchange*, discusses methods for performing the backup and recovery of data using virtual copies.
- Chapter 9, *Remote Copy for Recovery Manager*, provides instructions on using 3PAR Remote Copy with Recovery Manager.
- Appendix A, *Server Virtualization Environments*, provides instructions for creating environments for VMWare and Egenera.
- Appendix B, *Troubleshooting*, lists some common issues that may arise and suggested solutions for helping solve the problems.
- Appendix C, *Event Messages*, lists events, provides descriptions and describes possible actions.
- This guide also contains an index for your reference.

1.4 Typographical Conventions

The following typographical conventions are used in this guide:

Typeface	Meaning	Example
ABCDabcd	Used for dialog box elements such as titles and button labels.	Enter your system name in the **Value** box and click **OK**.
ABCDabcd	Used for file names, paths, and screen output, and for text you are to enter.	`Found < 12 > 73G disks.` Enter `cli` at the Windows command prompt.
ABCDabcd	Used to contrast your input with system output.	`cli% removevv VV1` `Removing vv VV1.`
ABCDabcd **ABCDabcd**	Used for variables in file names, paths, and screen output, and variables in user input.	[root@(*systemID-nodeID*)root] `To continue Enter your system name ==>` **`systemname`**

1.5 Advisories

To avoid injury to people or damage to data and equipment, be sure to observe the cautions and warnings in this guide. ***Always be careful when handling any electrical equipment.***



NOTE: Notes are reminders, tips, or suggestions that supplement the procedures included in this guide.



CAUTION: Cautions alert you to actions that can cause damage to equipment, software, or data



WARNING: Warnings alert you to actions that can cause injury to people or irreversible damage to data or the operating system.

2 Overview of Recovery Manager

In this chapter

2.1 System Requirements 2.2

2.2 Features Supported 2.3

2.3 Features not Supported 2.4

2.4 What's New in Recovery Manger for Exchange 4.1.0 2.4

2.5 Microsoft Volume Shadow Copy Service 2.4

2.6 How VSS Works with Exchange 2.6

2.7 Supported VSS Components 2.7

2.8 Recovery Manager Requirements 2.7

2.9 Recovery Manager Layout 2.8

2.9.1 Centralized Backup Configuration 2.8

2.9.2 Single Host Backup Configuration 2.10

2.9.3 CCR Backup Configuration 2.10

2.9.4 The Server Relationship 2.12

2.1 System Requirements

The current version of Recovery Manager for Exchange supports Microsoft Exchange 2007 and requires that the proper components are installed on the Production and Backup Servers and that the appropriate licenses are available on the InServ Storage Server. For complete details on system configurations, see *Recovery Manager Layout* on page 2.8.

Exchange Server (Production)

- Microsoft Exchange Server
- 3PAR InForm CLI
- 3PAR VSS Provider
- Recovery Manager Agent component

Backup Server

- Microsoft Exchange management tools
- 3PAR InForm CLI
- 3PAR VSS Provider
- Recovery Manager Backup Server component

InServ Storage Server (licenses required)

- Virtual Copy
- VSS Provider for Microsoft Windows
- Recovery Manager for Exchange
- Remote Copy (Optional)



NOTE: For both Microsoft Exchange and platform-specific release levels, please refer to the latest InForm OS Configuration Matrix which can be accessed through the 3PAR Document Control System (DCS).

Snapshot space must be available on 3PAR Virtual Volumes. In order to take snapshots on 3PAR's base volume, the volume itself must have snapshot space allocated during the base volume creation. Please see the *3PAR InForm OS Command Line Reference* for information on

creating a base volume with snapshot capability, or assigning snapshot space after the base volume is created.

2.2 Features Supported

- Exchange online virtual copy creation using Volume Shadow Copy Service
- Supports Volume Shadow Copy Service "Full" backup type
- Virtual copy creation using 3PAR VSS Provider for Microsoft Windows
- Access to 3PAR InServ Storage Server via InForm CLI for Microsoft Windows
- Mount virtual copies on Recovery Manager installed Windows hosts with read/write permissions
- Unmount virtual copies
- Delete virtual copies
- Backup using Symantec NetBackup
- Restore using Symantec NetBackup
- Filecopy restores
- Volume promote restores
- Virtual copy creation of LCR databases where the active and passive copies both reside on a single InServ.
- Virtual copy creation of CCR databases where active and passive copies reside on a single or dual InServ Storage Servers with a single or dual Recovery manager backup servers where the second backup server connects to a secondary InServ at the remote site
- Recovery Manager GUI
- Recovery Manager CLI
- Supports virtual copy creation of local and remote Exchange servers
- Supports Single Copy Cluster for Exchange 2007
- Centralized virtual copy management with multiple Exchange servers

2.3 Features not Supported

- VSS backup types "Incremental", "Differential", "Copy" and "Log" are not supported
- A single Exchange server spanning different InServs
- All backup tools excluding Symantec NetBackup
- Access to 3PAR InServ Storage Server via SSH
- Create virtual copy on System Boot Volume
- Cross-domain Exchange server management
- Exchange CCR volumes can not exist in an RC group
- Cross InServ mounts (includes CCR dual InServ configurations). VSS snapshot backup on Exchange 2007 for SCR node is not supported.

2.4 What's New in Recovery Manger for Exchange 4.1.0

This section contains information on the enhancements and new features available in the latest version of Recovery Manager for Exchange.

- Automatic synchronization of the Recovery Manager for Exchange repository and InServ is provided via the Recovery Manager for Exchange Graphical User Interface (GUI) and Command Line Interface (CLI).
- Automatic detection of asynchronous periodic Remote Copy resynchronizations allows periodic and manual synchronizations to occur without conflict.
- Synchronous Long Distance Remote Copy asynchronous periodic synchronization mode support.

2.5 Microsoft Volume Shadow Copy Service

Microsoft includes VSS (Volume Shadow Copy Service) in Windows to simplify the enterprise's storage environment. It provides a framework for creating a point-in-time copy of a single or multiple volumes.

Microsoft Windows Server VSS works with VSS-aware applications that are in use to determine when a volume shadow copy (snapshot) can be made. A snapshot is a copy of some data set,

for example, a disk volume, at a point in time. VSS then communicates with the operating system and applications and freezes computing tasks to allow snapshot creation. Without the freeze function, data could become corrupted when the snapshot is taken because the system might be in the middle of a task. Meanwhile, applications continue to run uninterrupted. The original volume continues to change as the process continues, but the shadow copy of the volume remains constant. VSS also gives permission to the backup application to access the volume and back it up in its "frozen" state. The shadow copy volume is then used for the actual backup. After the shadow copy volume is saved on the backup device, the shadow copy is deleted.

VSS coordinates between Requestors (backup applications – Recovery Manager), Writers (applications such as windows services – Exchange 2007) and Providers (components that create the shadow copies).

Table 2-1. VSS Components

VSS Component	VSS Component Description
Requestor	The requestor is backup software that initiates the creation of the shadow copy.
Writer	The writer is any application software that participates in the shadow copy process and whose files and data are included in the process.
Provider	The provider is the storage technology that does the actual shadow copy.

3PAR Confidential

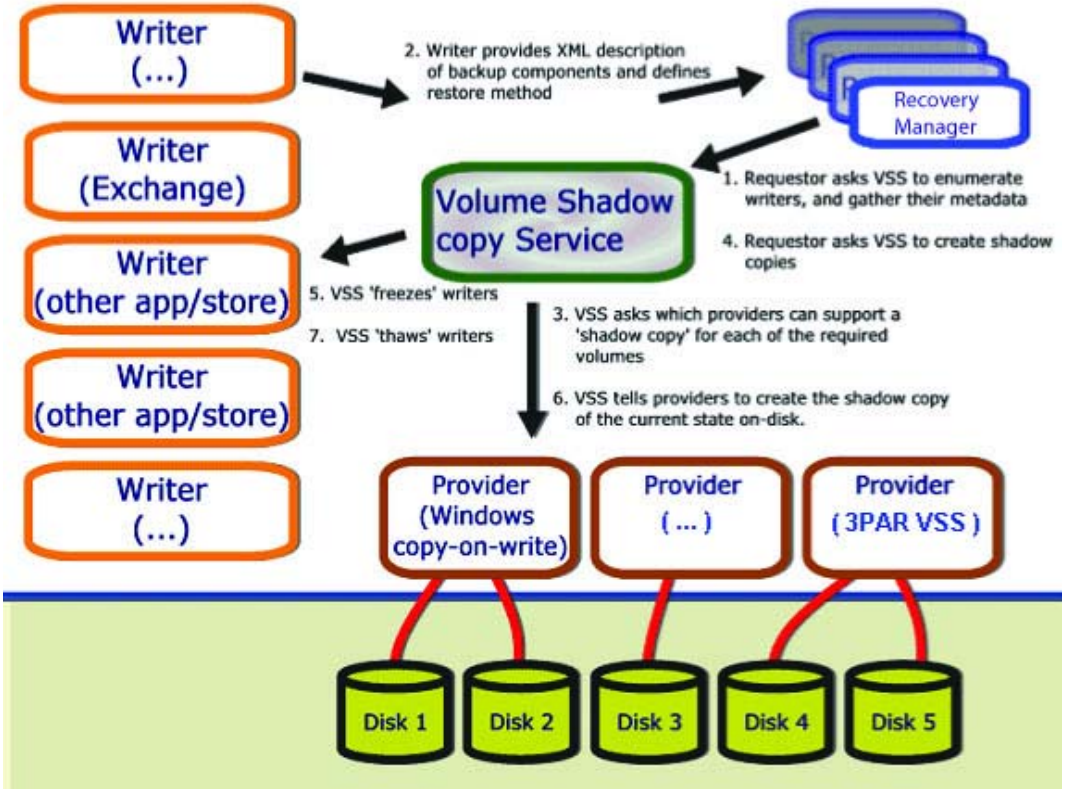


Figure 2-1. 3PAR VSS Provider for Microsoft Windows Operation Overview

2.6 How VSS Works with Exchange

1. The requestor (Recovery Manager) sends a command to the Volume Shadow Copy service to take a shadow copy of the selected Exchange storage group.
2. The Volume Shadow Copy service communicates with the Exchange writer to flush the current log file generation to disk and suspend any writes to the log files and to the .edb file. The .stm file will not be allowed to grow, however read-only access is still allowed. So anything that is already there can still be accessed from the client.
3. Volume Shadow Copy service communicates with the provider to initiate the shadow copy process for the disk volumes that contain Exchange data. VSS talks to the writers and

providers to fix a point in time for the shadow copy to take place; it is the provider that actually does the shadow copy.

4. The shadow copy typically takes less than a minute. Clients that use Microsoft Outlook in cached mode will not notice any disruption. Clients of earlier versions of Outlook may see the hourglass for several moments during the shadow copy process.
5. When the shadow copy has been taken, Volume Shadow Copy service communicates with the Exchange writer to let it know that it can resume writing to disk.
6. The queues of e-mail transactions are written to the logs.
7. The shadow copy is now available to the requestor for backing up.

2.7 Supported VSS Components

VSS components currently supported by 3PAR Provider for Microsoft VSS include:

- Requestor
  - Recovery Manager
  - Symantec NetBackup™ by Symantec for Windows
- Writer - Microsoft Exchange 2007



NOTE: For Symantec NetBackup supported version and Microsoft Exchange Server specific release levels, please refer to the latest InForm OS Configuration Matrix (PN 320-200099) which can be accessed through the 3PAR Document Control System (DCS).

2.8 Recovery Manager Requirements

- The Exchange Datastores for which virtual copies will be taken must be online.
- The same level of software updates is required on all Exchange servers.
- Microsoft Exchange System Management tools is required on the Backup Server.



NOTE: If you are running a Single Copy Cluster (SCC) or a CCR (Cluster Continuous Replication) on Windows 2008, the backup server needs to have the "Failover Clustering" feature enabled to function properly.

- Microsoft .Net Framework V3.5 and above is required. (This is a 3PAR VSS Provider requirement.)
- Visual C++ (2005 Redistributable) Runtime libraries (x64 or x86). This can be automatically installed by running the `Setup.exe` program provided with Recovery Manager for Exchange. (There is a known issue for Recovery Manager for Exchange when running `Setup.exe` on Windows 2008. If you have already installed the Visual C++ Runtime library, it will still ask you to install it again. You may install it again or directly install from the .msi file.)
- 3PAR VSS Provider 1.6.2 for Microsoft Windows.
- For CCR configurations on two InServs, where both nodes are separated over a long distance, two Recovery Manager for Exchange backup servers are required.



NOTE: For software-specific version support, see the latest 3PAR InForm OS Configuration Matrix, which can be found on the Document Control System (DCS).

2.9 Recovery Manager Layout

Recovery Manager provides two types of configuration depending on your environment setup: a centralized backup configuration and a single host backup configuration as described in the following sections.

2.9.1 Centralized Backup Configuration

A centralized backup configuration, as shown in Figure 2-2 on page 2.9 allows you to maximize the resources and performance of the Exchange servers through off-host central control management capabilities. A single backup server can remotely create virtual copies on multiple Exchange servers and manage all virtual copies on the backup server. This type of configuration is recommended if you need to manage multiple Exchange servers or are in a clustered environment.

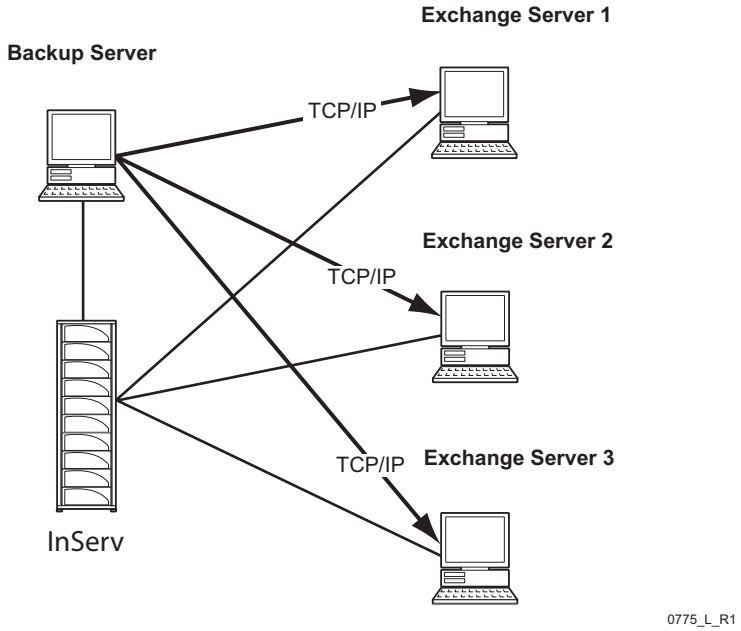


Figure 2-2. Centralized Backup Configuration

NOTE: The Exchange System Management Tools is required on the Recovery Manager Backup Server for Exchange database for validation purposes. In addition, the Exchange Servers and the Management Tools must utilize matched release and service pack versions.

NOTE: All the Exchange servers, including the Recovery Manager Backup Server component, must be in the same Windows domain.

2.9.2 Single Host Backup Configuration

A single host backup configuration, as shown in Figure 2-3, allows you to manage virtual copies locally on the Exchange server.

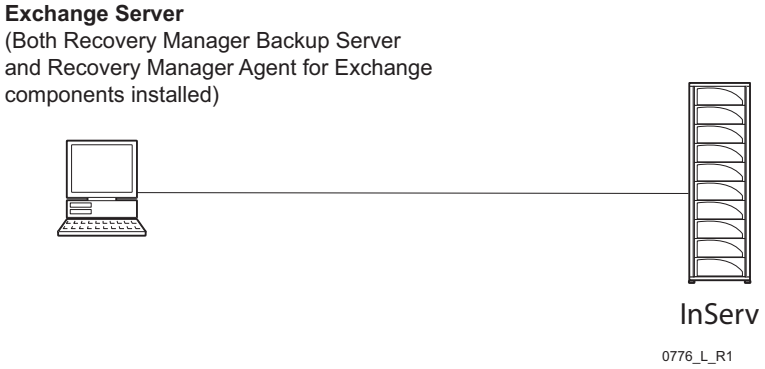


Figure 2-3. Single Host Backup Configuration

2.9.3 CCR Backup Configuration

CCR configurations can be implemented at a single site or span multiple sites. When implemented at a single site, a single backup server is utilized as shown in Figure 2-4 on page 2.11. For implementations that span multiple sites, two backup servers are required as shown in Figure 2-6 on page 2.12. The command `RMExch peer` is used to specify the name of the peer backup server for multiple sites. This command must be run in CCR configurations using two backup servers and is not required for CCR configurations using only one backup server. See Chapter 4, *Configuring Recovery Manager*.

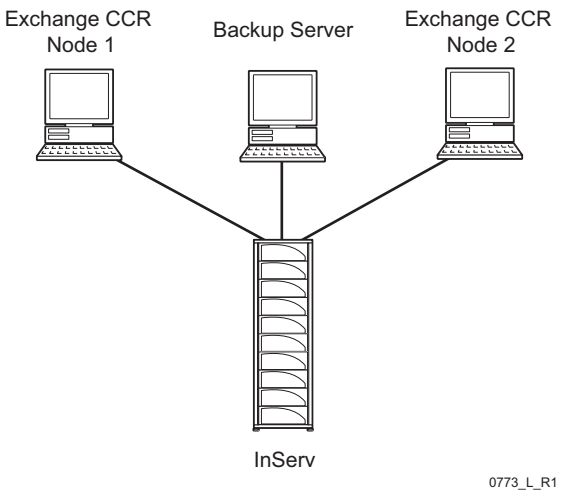


Figure 2-4. Single InServ, Single Site

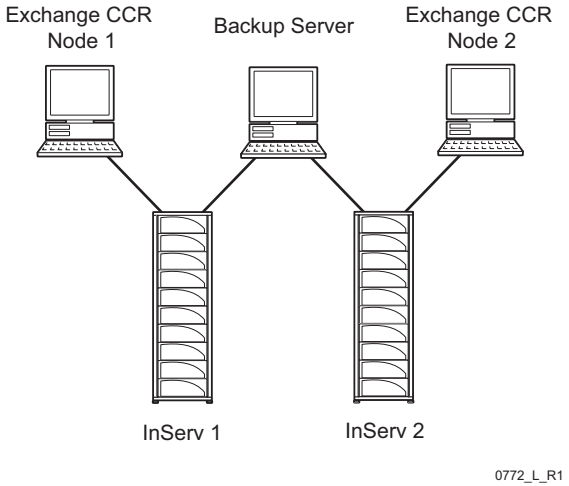


Figure 2-5. Two InServs, One Site

3PAR Confidential

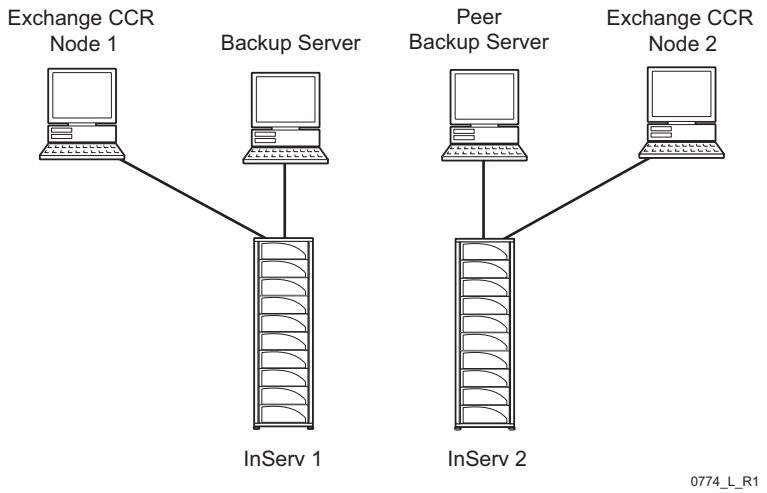


Figure 2-6. Two InServs, Two Sites

2.9.4 The Server Relationship

The following defines the roles and relationship between the server types:

Backup Server:

- The Backup Server plays a central control point for the Recovery Manager that controls and manages the backup and restore on different Exchange servers.

Exchange Servers:

- The Exchange Servers can be standalone servers or cluster virtual servers.

Connectivity:

- Both the Backup Server and Exchange Servers need to be connected to the same InServ. To manage a CCR-enabled configuration from a single backup server for CCR nodes that connect to two InServs within the same site; the backup server needs to connect to two InServs with separate FC or iSCSI connections. The InServs also need to be in the same active directory domain.

3 Installation and Deinstallation

In this chapter

3.1 Upgrading to Recovery Manager for Exchange **3.2**

3.1.3 Installing Recovery Manager **3.3**

3.2 Verifying the Installation **3.5**

3.5 Deinstalling Recovery Manager **3.7**

3.3 Understanding the Registry **3.5**

3.4 Environment Variables **3.7**

3.5 Deinstalling Recovery Manager **3.7**

3PAR Confidential

3.1 Upgrading to Recovery Manager for Exchange

This section provides instructions for upgrading to Recovery Manager for Exchange from version 2.2.4 through 3.0.2 to version 4.1.0.



NOTE: In Recovery Manager for Exchange, version 3.0.2, the installation directory has changed from `\Program Files\3PAR\vcdba\Exchange` to `\Program Files\3PAR\RM\Exchange`. To migrate from 2.2.4 or 3.0.1 to 3.0.2, deinstall RME, install RME 3.0.2, and move the Repository folder from the old `\vcdba\Exchange\Repository` to the new `\RM\Exchange\Repository` location.

3.1.1 Production Server

1. Deinstall Recovery Manager for Exchange. See section *Deinstalling Recovery Manager* on page 3.7.
2. Install Recovery Manager for Exchange 4.1.0. See section *Installing Recovery Manager* on page 3.3.

3.1.2 Backup Server

1. Backup the repository to a safe location, i.e. the folder `Exchange\Repository` and all directories and files under it.
2. Deinstall Recovery Manager for Exchange. See section *Deinstalling Recovery Manager* on page 3.7.
3. Install Recovery Manager for Exchange 4.1.0. See section *Installing Recovery Manager* on page 3.3.
4. Move the Repository folder from the old `\vcdba\Exchange\Repository` to the new `\RM\Exchange\Repository` location.
5. Check to see that the old virtual copies can be seen from the GUI and re-register the Exchange Server(s) if necessary.

3.1.3 Installing Recovery Manager

Before installing Recovery Manager, install the InForm OS Command Line Interface (CLI) for remote clients. For details on installing the CLI, see the *3PAR InForm OS Command Line Interface Reference*. You must also install the 3PAR VSS Provider application before installing Recovery Manager for Microsoft Exchange. Install Recovery Manager for Exchange on a host computer where Microsoft Exchange is running.



CAUTION: Do a backup of your data before upgrading the Recovery Manager or all data will be lost. See *Upgrading to Recovery Manager for Exchange* on page 3.2 for instructions on performing a backup.



NOTE: If you are installing the application through a remote desktop session, the newly added environment variables will not become effective until you log off the session. It is recommended that you install the application directly from the system console.



WARNING: Before installing Recovery Manager, create a backup of your repository data.

To install Recovery Manager:

1. Log on as the System Administrator.



NOTE: You must have Exchange server and system administrator rights.

2. Insert the Recovery Manager CD into a CD-ROM drive.
3. Open a Windows Explorer window:

   Click **Start** > **All Programs** > **Accessories** > **Windows Explorer**.
4. Click the CD-ROM drive to expand the files.
5. Double-click **Setup.exe**.

Result: Recovery Manager installation wizard launches.

6 Click **Next**.

Result: The **License Agreement** window appears.

7 Agree to the license, then click **Next**.

Result: The **Select Installation Folder** window appears.

8 Specify the installation directory for Recovery Manager.



NOTE: The **Disk Cost** button analyzes the amount of available storage space and compares it to the amount required for the Recovery Manager installation.

9 Click **Next** to confirm the installation destination.

Result: The **Select Recovery Manager Installation Type** window appears.

10 Specify the installation type for the local system.

- **Recovery Manager Backup Server** installs components required for local system to perform centralized backup management.
- **Recovery Manager Agent for Exchange Server** installs components for local system to be managed by the Recovery Manager Backup Server component installed server.
- **All of above** is for a single host setup where the local system manages its own virtual copies.

11 Click **Next** to confirm the local server selection.

Result: The **Confirm Installation** window appears.

12 Click **Next** to start the installation.

13 Click **Close** upon the completion of installation.

After closing, the system configuration information is gathered and displayed in a text file named `RMECfgChk.txt`. This information is useful for verifying whether all the required components are present on the system.



NOTE: When using a remote desktop connection, log off as Admin and then log on again to update the path before starting to use Recovery Manager.

3.2 Verifying the Installation

Verify the Recovery Manager installation as follows:

1. Log on as the System Administrator.
2. Click **Start** > **Control Panel** > **Add/Remove Programs**.

   Result: The **Add/Remove Programs** window appears.
3. Verify Recovery Manager appears under the **Currently installed programs** column.

3.3 Understanding the Registry

After Recovery Manager is installed successfully, some information is written into the registry database under: `HKEY_LOCAL_MACHINE\SOFTWARE\3PAR\RM_Exchange`.



CAUTION: DO NOT try to edit the registry key value unless asked by your local service provider for support purposes.



NOTE: For tracking purposes, you will be asked to modify the value of **TraceLevel** to a higher number to record more detailed information to the log file.

The Tracelevel has the following values:

- 1 - Error messages logged.
- 2 - Error and warning messages logged.
- 3 - Error, warning, and informational messages logged.
- 4 - Error, warning, informational and debug messages logged.
- 5 - Error, warning, informational, debug and verbose messages logged.

To edit registry data for Recovery Manager:

1. Click **Start** > **Run**, then enter **regedit** in the **Run** window and click **OK**.

   Result: The **Registry Editor** window displays:

2 Expand **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **3par** > **RM_Exchange** from the left-side of the window.

3 Double-click **TraceLevel** from the right-side of the window.

Result: The **Edit Value** popup appears.

4 Modify the **Value Data** field and click **OK** to save the change.

Table 3-1. System Registry Values for Recovery Manager

Name	Value
BackupTimeout	The timeout value for the NetBackup initialization process detection in minutes. This setting is optional if the default is not appropriate.
GUILog	Location of the GUI Log File (java errors only).
InstallPath	Recovery Manager Installation path.
JarPath	Path to the GUI jar file.
RCQueryTimer	The monitoring interval for remote copy progress on the target server in minutes. This setting is optional if the default is not appropriate.
RepPath	Root path to the Recovery Manager repository.
TraceHistory	Number of Trace files to keep before deleting.
Tracelevel	The trace level for the log file: 1 Error Messages 2 Warning Messages 3 Informational Messages 4 Debug Messages 5 Routines called The default value is set to "5".
TraceLog	The location where the log file resides.



NOTE: See *Event Messages* on page C.11 for descriptions of events and possible actions to fix possible problems.

3.4 Environment Variables

Installation of Recovery Manager adds the full path to its executables and libraries to the systems PATH environment variable. If for some reason this has not been done, the GUI or CLI will not work. If this is the case, manually add the full paths for the `bin` and `ext` directories under **RM/Exchange** to the PATH environment variable.

3.5 Deinstalling Recovery Manager



CAUTION: Perform a backup of your data before upgrading the Recovery Manager or all data will be lost. See *Upgrading to Recovery Manager for Exchange* on page 3.2 for instructions on performing a backup.

To deinstall Recovery Manager from Windows 2008:

1. Log on as the System Administrator.
2. Click **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.

   Result: The **Add/Remove Programs** window appears.
3. Select **3PAR Recovery Manager for Microsoft Exchange.**
4. Click **Uninstall**.



NOTE: Removing Recovery Manager installation will not remove the Recovery Manager repository for virtual copy management.

4 Configuring Recovery Manager

In this chapter

4.1 Configuring the Database 4.2

4.2 Configuring Recovery Manager's Installation Location 4.2

4.3 Configuring Recovery Manager's Search Path 4.2

4.4 Configuring the Host Computer and the 3PAR InServ Storage Server 4.2

4.5 Configuring Recovery Manager Communications 4.2

4.6 Configuring the Policy for an Exchange Server 4.3

4.7 Configuring Recovery Manager for CCR 4.4

4.1 Configuring the Database

The system supports Microsoft Exchange 2007 files created on basic disks using the NTFS file system.



NOTE: 3PAR recommends that each mailbox or public store, (as well as log files), be allocated to separate volumes. This configuration provides the greatest flexibility when performing individual mailbox or mailbox store recovery, thus reducing the exposure to conflicts between mailbox data stores.

4.2 Configuring Recovery Manager's Installation Location

By default Recovery Manager is installed in `%SystemDrive%\Program Files\3PAR\RM\Exchange`.

4.3 Configuring Recovery Manager's Search Path

The Recovery Manager executables are stored in the program folders directory chosen during installation. To use the command line components, the Recovery Manager directory must be added to the Windows Path variable. During installation, the search path is automatically added to the environment variable PATH.

4.4 Configuring the Host Computer and the 3PAR InServ Storage Server

See the *3PAR InForm OS Concepts Guide* and the *3PAR InForm OS CLI Administrator's Manual* for information about configuring the controller nodes on the InServ Storage Server to communicate with the host computer.

4.5 Configuring Recovery Manager Communications

- The Recovery Manager's listening service on each Recovery Manager Agent component installed on the Exchange server and Recovery Manager Backup Server communicate through a TCP/IP port.

- The default port value is 9933. You can change the port value using the RMExch `portconfig` command. When one host's port configuration is changed, all hosts associated in the centralized backup configuration must be changed to the same IP port with Recovery Manager for Exchange Agent service restarted.

For Example:

- To show the current configured port for the Windows host named spotted, open a command prompt and issue the `RMExch portconfig -h spotted` command.

```
Recovery Manager for Exchange, Version 4.1.0
Command: RMExch portconfig -h spotted
Current port: 9933
```

- To change the host's configured port to 9950, open a command prompt and issue the `RMExch portconfig -h spotted -p 9950` command.

```
Command: RMExch portconfig -h spotted -p 9950
Updated the local Port to 9950
```

- Restart the Recovery Manager for Exchange Agent service on each server you ran the command against.

4.6 Configuring the Policy for an Exchange Server

Recovery Manager uses a policy to maintain the maximum number of virtual copies created for each storage group.

For example:

- To see the current policy for a specific storage group (MyStorageGroup) of an Exchange server (spotted), open a command prompt and issue the `RMExch policy -s spotted -g MyStorageGroup` command.
- To change the policy to 15, open a command prompt and issue the `RMExch policy -s spotted -g MyStorageGroup -i 15` command.
- To change the policy to <n> and allow removal of the oldest virtual copy, open a command prompt and issue the `RMExch policy -s spotted -g MyStorageGroup -i <n> -r` command.



NOTE: The minimum number of virtual copies allowed is **1** and the maximum is **500**. The default is **10**.



NOTE: If a single backup server is managing active and passive nodes, the maximum virtual copy count mentioned in the policy will be enforced on each node separately. Hence, the backup server can have twice the number of maximum virtual copy count.

4.7 Configuring Recovery Manager for CCR

Recovery Manager for Exchange provides support for CCR. Depending on your CCR requirements, Recovery Manger for Exchange must be configured accordingly.

- If your CCR configuration utilizes a single InServ, you can rely on a single backup server and do not need to perform any additional configuration steps.
- If your CCR configuration spans two InServs, you will require two backup servers (one connected to each InServ). One will act as the backup server managed CCR active node and the other the peer backup server managed CCR passive node. Both backup servers can execute RMExch commands.

To configure Recovery Manager for CCR on two InServs with two backup servers, use the `RMExch peer` command to configure the peer backup server as described in *RMExch peer* on page 7.17. You can use the `RMExch peer display` command to display the current configuration.

Additionally, you will need to configure the provider to use the InServ that each backup server and Exchange production will connect to. This is done through the provider's `ProvCfg.exe` utility (refer to the provider's user's guide for details). If your CCR configuration has one InServ, then add only that one InServ using the `ProvCfg.exe` utility. If your CCR configuration has two InServs at one site, you will need to add both InServs to your backup server. If your configuration has two InServs at two sites, you need to add one InServ to each backup server. See Chapter 2, *Overview of Recovery Manager*, *CCR Backup Configuration* on page 2.10 for the appropriate configuration diagrams.

5 Configuring NetBackup for Recovery Manager

In this chapter

5.1 Overview 5.1

5.2 Defining a NetBackup Policy 5.2

This chapter contains instructions for configuring Symantec NetBackup for use with Recovery Manager.

5.1 Overview

Recovery Manager can be used with Symantec NetBackup for the backup and restore of virtual copies created by Recovery Manager. There should be two NetBackup master servers for CCR configurations that span two sites (and two InServs). The following sections describe setting up Symantec NetBackup for use with Recovery Manager.



NOTE: Refer to the latest InForm OS Configuration Matrix located in the 3PAR Document Control System (DCS) for supported versions of Symantec NetBackup.

5.2 Defining a NetBackup Policy

Follow these instructions to setup a NetBackup policy for use with Recovery Manager.



NOTE: A storage unit to store the virtual copy backups should already be set up. See the Symantec NetBackup documentation for setting up a storage unit.

1. Launch the Symantec **NetBackup Administration Console**.
2. Right-click the **Policies** node in the left pane to open the drop-down menu.
3. Double-click **New Policy...** from the drop-down menu.

   Result: The **Change Policy** window appears.
4. On the **Attributes** tab:
   a. Select **MS-Windows-NT** from the Policy type menu.
   b. Select the storage unit where the virtual copy backups will reside from the Policy storage unit menu.
5. Select the **Schedules** tab and click **New...**

   Result: The **Change Schedule** window appears.
6. On the **Attributes** tab:
   a. Enter a name for the schedule in the **Name** box.
   b. Select **Full Backup** from the Type of backup drop-down menu.

      Select **User Backup** if you are using the NetBackup client interface from the machine where the Recovery Manager Agent for Exchange Server component is installed.
7. Select the **Start Window** tab.
8. Activate all the time slots by selecting from the drop down menus:
   - Modify Day: **Mon**
   - Start Time: **12:00:00AM**
   - End Day: **Sun**
   - End Time: **12:00:00AM**

- Duration (days): **7**

9 Click **OK** to return to the **Change Policy** window and to activate the schedule.

10 Select the **Clients** tab from the **Change Policy** window.

11 Enter the machine name where the Recovery Manager Backup Server component is installed.

12 Click **OK** to confirm the client setup.



NOTE: Recovery Manager supports full backups when running with a NetBackup Master server. Recovery Manager also supports the user backup when running with a NetBackup client machine.



NOTE: When using NetBackup with Recovery Manager for Exchange and VSS, the NetBackup client may take an additional temporary read-only and read/write snapshot on your base volumes. This behavior can either be ignored or turned off by disabling the **Windows Open File Backup** in NetBackup.



NOTE: If you plan on backing up multiple storage groups using NetBackup and Recovery Manager for Exchange, you need a different policy for each storage group that will be backed up at the same time. For example, if the first backup of Storage Group One has not finished yet, in order for the backup of Storage Group Two to be performed correctly by Recovery Manager for Exchange and Netbackup, it must use a different policy.

3PAR Confidential

6 Using the Recovery Manager GUI

In this chapter

6.1 Overview of the Recovery Manager GUI 6.2

6.1.1 Menu Bar 6.3

6.1.2 Node Tree Pane 6.4

6.1.3 Informational Right Pane 6.4

6.1.4 Displaying Server Information 6.4

6.1.5 Displaying Storage Group Information 6.4

6.2 Starting the GUI 6.6

6.3 Stopping the GUI 6.6

6.4 Server Registration 6.6

6.5 Setting Recovery Manager Policy Configuration 6.6

6.6 Creating a Virtual Copy 6.7

6.6.1 To Create a Virtual Copy of a Storage Group 6.8

6.6.2 Create a Remote Virtual Copy 6.8

6.6.3 LCR Virtual Copy 6.8

6.6.4 CCR Virtual Copy 6.9

3PAR Confidential

6.7 Mounting a Virtual Copy 6.10

6.8 Unmounting a Virtual Copy 6.11

6.9 Refreshing Virtual Copy Information 6.11

6.9.1 Refreshing all Virtual Copies 6.11

6.9.2 Refreshing all Virtual Copies for a Specific Storage Group 6.11

6.9.3 Refreshing a Specific Virtual Copy 6.11

6.10 Backing up a Virtual Copy Using Symantec NetBackup 6.11

6.10.1 Backup at the Storage Group Level 6.12

6.10.2 Backup at the Storage Group Level for CCR 6.12

6.11 Restoring from Virtual Copy Timestamp 6.14

6.11.1 File Copy Restore 6.14

6.11.2 Volume Restore 6.14

6.12 Restoring a Virtual Copy Using Symantec NetBackup 6.15

6.13 Removing a Virtual Copy 6.16

6.14 Virtual Copy Status 6.17

6.15 Event Messages 6.17

6.16 Analyzing the Repository 6.17

6.17 Validating a Virtual Copy 6.18

This chapter provides instructions for using the Recovery Manager Graphical User Interface (GUI) to back up and restore storage groups.

6.1 Overview of the Recovery Manager GUI

Recovery Manager provides a Graphical User Interface (GUI) to backup and restore storage groups at a point-in-time. The Recovery Manager GUI is a windows application, containing a menu bar, a node tree pane, informational right pane and a command log window. It provides the capability to create, remove, mount, and unmount, backup and restore the virtual copy for a storage group.

NOTE: The GUI will not be available for Recovery Manager Agent for Exchange Server installations.

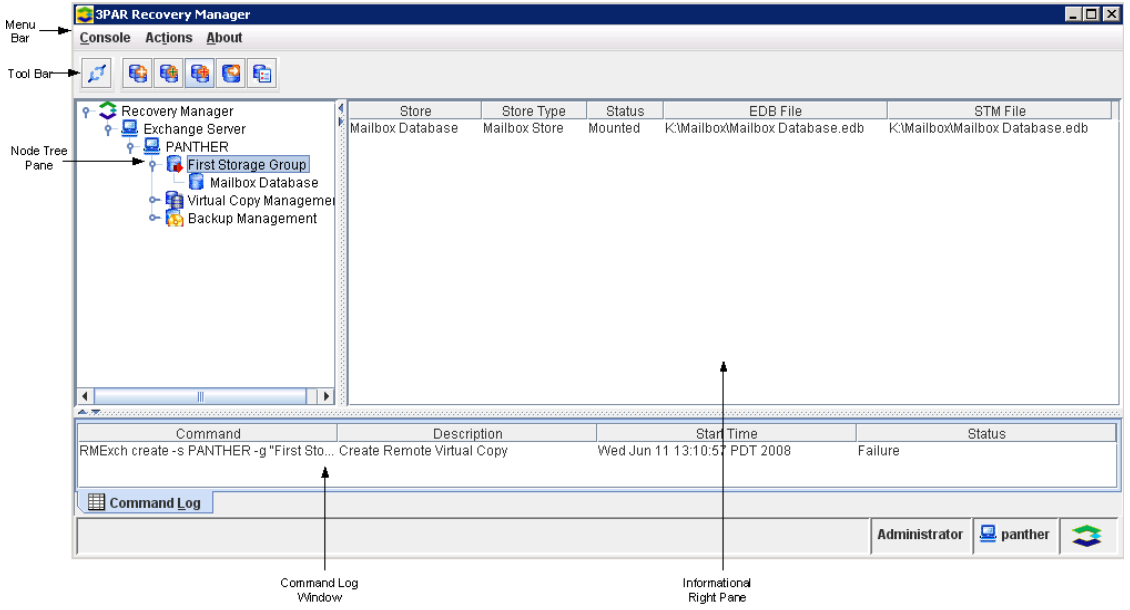


Figure 6-1. GUI Overview

6.1.1 Menu Bar

The menu bar consists of the following menu items:

- **Console** menu - allows you to exit the GUI and register the server.
- **Actions** menu - allows you to access virtual copy functionality.
- **About** menu - provides an **About 3PAR Recovery Manager** screen and access to other helpful links such as descriptions for event messages may be generated during operation.

6.1.2 Node Tree Pane

The node tree presents the system's Exchange server. When the Recovery Manager GUI starts, it analyzes the servers' storage groups, mailbox information, and virtual copies, then displays them graphically as a nested tree in the left pane.

6.1.3 Informational Right Pane

The right pane displays detailed information about each item selected in the node tree pane. The information displayed in the right pane is presented in columns. A scroll bar is provided at the bottom of the pane should the pane's contents exceed the pane's width.

6.1.4 Displaying Server Information

Recovery Manager supports feature Local Continuous Replication (LCR) and Cluster Continuous Replication (CCR). LCR and CCR enabled storage groups are marked with the  and  icons and correspondingly in the node tree pane. A **LCR/CCR** column is added in the informational pane to show which storage group is LCR/CCR enabled. Performing a **Rescan Server Configuration** is required in order to view the updated LCR/CCR status icon.

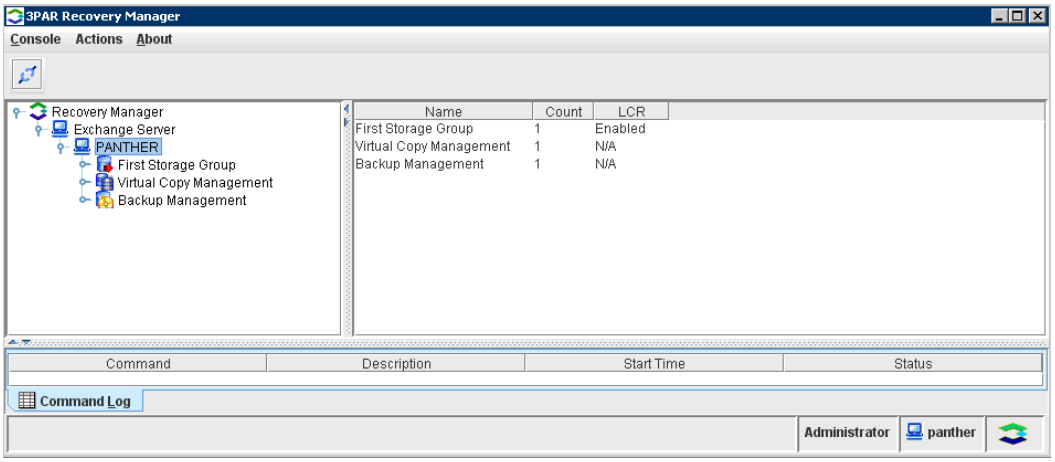


Figure 6-2. Displaying Server Information

6.1.5 Displaying Storage Group Information

To display information about a particular storage group, click on the storage group name in the node tree. Detailed information about the selected storage group is displayed in columns in the right pane.

The following figure displays storage group information for the selected storage group "**First Storage Group**".

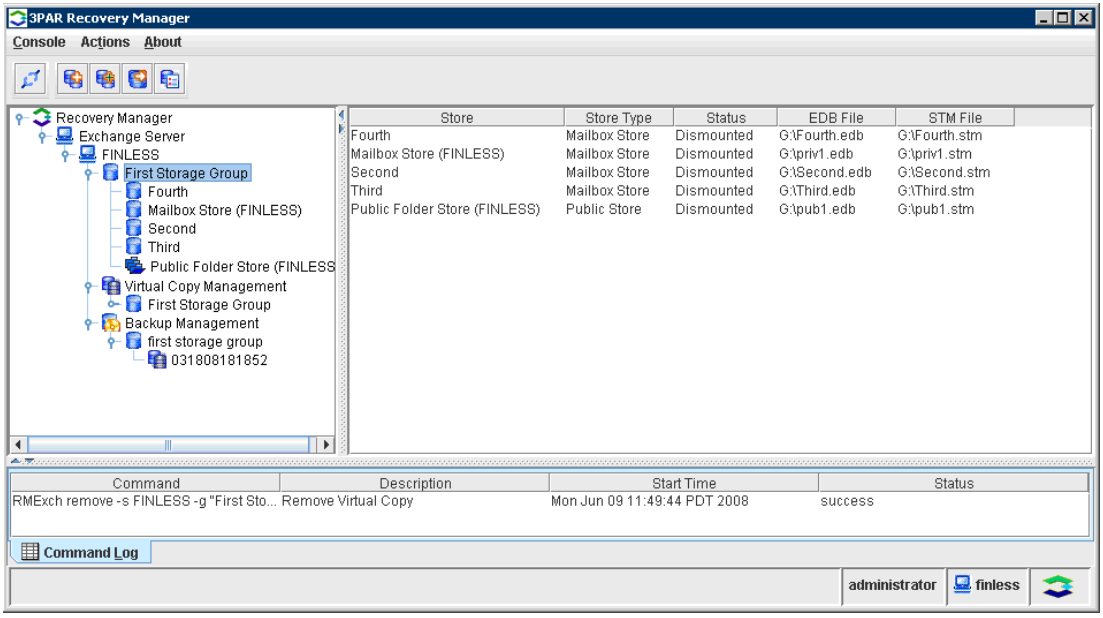


Figure 6-3. Displaying Storage Group Information

Table 6-1. Explanation of Columns

Column...	Provides...
Store	The name of the information store.
Store Type	The type of information store; either **Mailbox Store** or **Public Store**.
Status	The status of the data store; either **Mounted** or **Unmounted**.
EDB File	The location of the EDB (property store) file store.

6.2 Starting the GUI

To start the Recovery Manager GUI, locate and double-click the **3PAR Recovery Manager for Exchange** icon on your desktop.

6.3 Stopping the GUI

To stop the Recovery Manager GUI, on the menu bar, click **Console** > **Exit**. For additional information, see *Menu Bar* on page 6.3.

6.4 Server Registration

Before the GUI can manage Exchange Servers, all servers have to be registered. To register a server, right click the **Exchange Server** node and select **Server Registration**.

All Exchange servers on the same domain will be shown. Click any server, which is managed by the Recovery Manager GUI for Exchange, and click **OK**.



NOTE: Recovery Manager will take a few minutes to scan all Exchange Servers. It may take longer the first time this operation is performed.



NOTE: When a new instance or a new Storage Group is created after the server registration, server configuration has to be rescanned before it can be managed by Recovery Manager. To rescan, right-click the **Exchange Server** node and select **Rescan Server Configuration**.

6.5 Setting Recovery Manager Policy Configuration

By default, Recovery Manager creates a maximum of 10 virtual copies per storage group. Recovery Manager provides a policy setting feature which allows you to set the maximum number of virtual copies permitted per storage group on the current Exchange server.

The policy setting is applied at the storage group level allowing each storage group to have its own policy configuration.

When setting the virtual copy limit, you can also optionally select the **Remove Old Virtual Copies** radio button indicating that the oldest virtual copy for each storage group is automatically removed once the set maximum limit of virtual copies is reached.



NOTE: If the oldest virtual copy is mounted, a snapshot will not be created until it is unmounted.

If the **Remove Old Virtual Copies** checkbox is unselected, once the set maximum limit is met, a new virtual copy cannot be created until you manually delete any old virtual copies.

To set Recovery Manager policies:

1. Start Recovery Manager (see *Starting the GUI* on page 6.6).
2. Select the storage group that is to be configured in the node tree pane.
3. Right-click the storage group and select **Policy**.

   Result: The **Recovery Manager Policy** dialog box appears.
4. Enter the **Maximum virtual copies kept in InServ** in the text field.
5. If you want to remove the oldest virtual copy, select **Remove the oldest virtual copy** option. If you want to keep the oldest virtual copy, select **Retain the oldest virtual copy** option.
6. Click **OK**.



NOTE: The virtual copy policy is effective immediately.

6.6 Creating a Virtual Copy

Virtual copies are created at the storage group level for Microsoft Exchange Server, since this is the recoverable unit defined by Microsoft. The log files for all the mailbox data stores in a storage group are managed at the storage group level. Therefore, when Recovery Manager creates a virtual copy for a Microsoft Exchange storage group, it creates a virtual copy of all virtual volumes where the information store, log, and system files reside to preserve the data

for consistency. A virtual copy can also be created and saved in a remote server which is called create remote virtual copy.

6.6.1 To Create a Virtual Copy of a Storage Group

1. Navigate through the node tree view on the left pane and locate the storage group for which a virtual copy is to be created.
2. Right-click the storage group name and select **Create** > **Virtual Copy**.



NOTE: A virtual copy can only be taken of a storage group that is online.



NOTE: Creating a virtual copy of a storage group creates a virtual copy of all the volumes where the storage group data (logs, chk, and edb files) resides. Therefore, it is recommended that volumes storing exchange data files are not used to store any other data.

Once a virtual copy is created, it appears under the **Virtual Copy Management** node under the relevant storage group name. The virtual copy is given a timestamp that is used as its name.

6.6.2 Create a Remote Virtual Copy

To create a remote virtual copy of a storage group:

1. Navigate through the node tree view on the left pane and locate the storage group for which a virtual copy is to be created.
2. Right-click the storage group name and select **Create** > **Remote Virtual Copy**.

6.6.3 LCR Virtual Copy

A Local Continuous Replication (LCR) can be created to replicate the storage group. Creating a LCR Virtual Copy will use the LCR as source to create the Virtual Copy. Similar to regular Virtual Copy, the log files for all the mailbox data stores in a storage group are managed at the storage group level. Therefore, when Recovery Manager creates a virtual copy for a Microsoft

Exchange storage group, it creates a virtual copy of all virtual volumes where the information store, log, and system files reside to preserve the data for consistency.

To create a LCR virtual copy of a storage group:

1. Navigate through the node tree view on the left pane and locate the LCR enabled storage group for which a virtual copy is to be created.
2. Right-click the storage group name select **Create** > **LCR Virtual Copy**.

6.6.4 CCR Virtual Copy

A Cluster Continuous Replication (CCR) Virtual Copy can be created to replicate the storage group. You can create the Virtual Copy for an Active Node, Passive Node, and Passive and Active Node. A Virtual Copy is created based on the resource from the Active node of the cluster and saved to the Active node corresponding backup server (primary).

- Create Virtual Copy on a Passive Node will gather its resource from the Passive node of the cluster and save it to the Passive node corresponding backup server.
- Create Virtual Copy on a Passive and Active node will create the Virtual Copy on the Passive node as above, then create the Virtual Copy on the Active node as above.

To create a CCR Virtual Copy of a storage group:

1. Navigate through the node tree view on the left pane and locate the CCR enabled storage group for which a Virtual Copy is to be created.
2. Right-click the storage group node and select **Create** > **CCR Virtual Copy on Active Node**, **Create** > **CCR Virtual Copy on Passive Node**, or **Create** > **CCR Virtual Copy on Passive and Active Node**.



NOTE: The Production Server VSS will wait for up to 10 seconds for the writers to freeze I/O; this interval is not configurable. In most cases 10 seconds is a sufficient window to successfully create a virtual copy. However, in some circumstances under very heavy load, 10 seconds may not be enough and the virtual copy will fail on this attempt, which is by design. VSS does not automatically retry the shadow copy creation, you must retry the virtual copy creation using the Recovery Manager GUI or the command line.



NOTE: On the Production Server during virtual copy creation, Recovery Manager dismounts and unmasks the virtual copy device from the Windows server, and breaks the virtual copy away from VSS control. During this process a delayed write error may appear, or the message **the system failed to flush data to the transaction log** may appear in the System Event Log. This is normal.



NOTE: Recovery Manager checks the integrity of the Exchange files after creating a virtual copy. A manual check may be performed as well.



NOTE: If the active node and passive node pair under the CCR setup get switched (failover), select **Console** > **Rescan Server Config** to update the tree information. However, the cluster failover may temporarily cause the Exchange storage group to be in an Initializing state for a few seconds. Wait until it returns to a healthy state before starting the rescan.

6.7 Mounting a Virtual Copy



NOTE: A virtual copy may only be mounted to one host at a time.

A virtual copy can be mounted at the timestamp level. Once a timestamp is mounted, all stores (mailbox, public store, logs) under the timestamp are mounted.

To mount an individual store:

1. Right-click on the timestamp in the left pane node tree view and select **Mount**.

   Result: The select host dialog, listing the available host names identified to the associated InServ appears.

2. Select the host to mount the virtual copy (store) to, from the host name drop down box.
3. Click **OK**.

Result: The virtual copy is available to the selected host server. The list view in the right pane is updated for the mounted virtual copy (store). The virtual copy status shows **Mounted** and the mounted host column shows the host server to which the virtual copy was mounted.

6.8 Unmounting a Virtual Copy

A virtual copy can be un-mounted at the timestamp level. Once a timestamp is unmounted, all stores (mailbox, public store, logs) under the timestamp are unmounted.

- To unmount a virtual copy at the timestamp level, right-click on the mounted store name in the left pane node tree view, and select **Unmount**.

  Result: The right pane list view is updated for the unmounted virtual copy it's status now shows **Unmounted** and the **Mounted Host** column is blank.

6.9 Refreshing Virtual Copy Information

Recovery Manager provides both GUI and CLI utilities. If both are used interchangeably without stopping and restarting the GUI, the virtual copy information needs to be updated. This can be done at several levels.

6.9.1 Refreshing all Virtual Copies

- To refresh all virtual copies, right-click the **Virtual Copy Management** node in the left pane node tree and select **Refresh**.

6.9.2 Refreshing all Virtual Copies for a Specific Storage Group

- To refresh all virtual copies for a specific storage group, right-click the storage group under the **Virtual Copy Management** node and select **Refresh**.

6.9.3 Refreshing a Specific Virtual Copy

- To refresh a specific virtual copy, right-click the virtual copy timestamp and select **Refresh**.

6.10 Backing up a Virtual Copy Using Symantec NetBackup

Recovery Manager allows backup of the virtual copies to media using Symantec NetBackup.

To backup a virtual copy using NetBackup, you must first configure Symantec NetBackup as described in Chapter 5, *Configuring NetBackup for Recovery Manager*.

A backup can be performed on the storage group level or the timestamp level.

6.10.1 Backup at the Storage Group Level

This backup is a fully automatic backup that creates a virtual copy for the storage group, mounts it, backs it up to media, unmounts it, and removes it automatically.

To backup a virtual copy at the storage group level:

1. Right-click the storage group node you wish to backup in the left pane node tree, then select **Backup to Media**.

   Result: The **Backup to Media** dialog box appears:

2. Enter the **Master Server Name**, the **NBU** policy name, and **NBU Full Schedule Name** in the text boxes provided. The policy and schedule names should be the names of the policy and schedule that were set up for use with Recovery Manager in Chapter 5, *Configuring NetBackup for Recovery Manager*.

3. (Optional) You can choose to remove the virtual copy from the InServ if the backup completes successfully by checking the check box labeled **Remove virtual copy from InServ after NBU backup**.

4. Click **OK**.



NOTE: You can monitor the NetBackup progress using the progress log, which reside at the following location:
`RM_Exchange Install Location\log\nbulog\exchserver_storagegroup_timestamp.log`

6.10.2 Backup at the Storage Group Level for CCR

Net Backup for CCR has two options, **Backup on Active Node** and **Backup on Passive Node**. Backup on the active node will create a Virtual Copy on the active node of the cluster and backup to the corresponding NetBackup server. Similarly, Backup on the passive node will create a Virtual Copy on the passive node of the cluster and backup to the corresponding NetBackup server.

To backup a Virtual Copy at the storage group level:

1 Right-click the storage group node you wish to backup in the left pane node tree, then select **Backup** > **on Active Node** or **Backup** > **on Passive Node**.

Result: The **Backup To Media** dialog box appears:

2 Enter the **Master Server Name**, the **NBU policy name**, and **NBU Full Schedule Name** in the text boxes provided. The policy and schedule names should be the names of the policy and schedule according to the Active node or Passive node that is selected.

The backup process will start on the corresponding backup server. When the Backup on Passive node is started on Backup Server1 with the **remove created Virtual Copy** checkbox unchecked, a Virtual Copy and a Backup Virtual Copy will be created and shown in the Backup Server2.

3 (Optional) You can choose to remove the virtual copy from the InServ if the backup completes successfully by checking the check box labeled **Remove virtual copy from InServ after NBU backup**.

4 Click **OK**.

The GUI is updated to show that the virtual copy has been backed up (see Table 6-2).

Table 6-2. Verifying the Virtual Copy Backup Status

Column	Value
Virtual Copy Status	If the option to remove the virtual copy from the InServ storage server after successful backup is selected, the status is **Removed**. If the virtual copy is not removed, the status shows **Mounted**. See *Virtual Copy Status* on page 6.17.
Backup Mechanism	NBU
Backup Type	FULL
Backup Keyword	Recovery Manager generated keyword for the NBU backup, format: exchange `server_storagegroup_timestamp`.

NOTE: If the backup fails, refresh the GUI to reset the above columns back to their previous values.

6.11 Restoring from Virtual Copy Timestamp

Recovery Manager allows restore of the virtual copy to its source storage group. A Virtual Copy Timestamp can be restored by using File Copy or Volume restore. The restore operation will restore from a mounted and un-mounted Virtual Copy Timestamp. A mounted timestamp  or non-Promotable timestamp  can only perform File Copy restore. A promotable timestamp  can perform both File Copy and Volume restore.

6.11.1 File Copy Restore

To perform a file copy restore:

1. Navigate through the node tree view on the left pane and locate the timestamp of the corresponding storage group.
2. Right-click the timestamp select **Restore Using** > **File Copy**.

   Result: The **File Copy Restore** dialog box appears:
3. Select **Click to continue** to confirm you understand the warning, then click **Ok**.

   Result: Only the modified data will be replaced with the data in the selected virtual copy.

6.11.2 Volume Restore

To perform a volume restore:

1. Navigate through the node tree view on the left pane and locate the timestamp of the corresponding storage group.
2. Right-click the timestamp and select **Restore Using** > **Volume**.

   Result: The **Volume Restore** dialog box appears:
3. Select **Click to continue** to confirm you understand the warning, then click **Ok**.

   Result: The whole volume of the storage group will be restored with the data in the selected virtual copy.



WARNING: DO NOT perform a volume promote restore if multiple storage groups share any volumes. This includes all data files .LOG, .EDB, and .CHK. If you are not sure how or if your storage groups share volumes, execute the `chk_multi_storage.cmd` script by default installed at `Program Files/3PAR/RM/Exchange/bin` to determine how any storage groups may be sharing volumes.

6.12 Restoring a Virtual Copy Using Symantec NetBackup

Once a virtual copy is backed up to media, the **Restore** menu option is enabled.

Backups can be restored back to their original location (the volume(s) or directory locations of the virtual copies that were backed up, not original exchange data locations), or an alternate location can be specified.

To restore a virtual copy that has been backed up using NetBackup:

1. Right-click the timestamp under Backup Management you wish to restore and select **Restore**.

   Result: The **Restore Virtual Copy from Media** dialog box ppears.

2. To restore to an alternate location, enter the location in the text box provided. To restore back to the original location, leave the text box as it is.



NOTE: To restore back to the original location, make sure the original location is still valid.

3. Click **OK**. The GUI assumes a successful restore. The NetBackup restore progress can be monitored using the progress log located at: `RM_Exchange Install Location\log\nbulog\exchserver_storagegroup_timestamp.log`

If an alternate restore location was specified, the restored data appears in the alternate location.

6.13 Removing a Virtual Copy



NOTE: A virtual copy cannot be removed if it is mounted to a host server.

To remove a virtual copy from the InServ and the Recovery Manager repository, the virtual copy timestamp must have a status of **Available**.

- To remove a virtual copy, right-click the virtual copy timestamp node and select **Remove**.

  Result: The virtual copy is removed from both the InServ and the Recovery Manager repository.

If the **Remove virtual copy from InServ after NBU backup** option was selected, the virtual copy only exists in the Recovery Manager repository for restore purposes. In this case the virtual copy will have a status of **Removed**.

- To remove the virtual copy from the Recovery Manager repository, right-click the virtual copy timestamp node and select **Remove Backup**.

  Result: The virtual copy is removed from the Recovery Manager repository.



WARNING: If a virtual copy is removed from the InServ Storage Server during a backup operation, then deleted from the Recovery Manager repository before a restore operation has taken place, all data is lost and will be unable to recover the storage group.

6.14 Virtual Copy Status

Table 6-3 describes each virtual copy status.

Table 6-3. Virtual Copy Status Descriptions

Virtual Copy Status	Description
Available	A virtual copy has this status when it exists in InServ Storage Server and in the Recovery Manager repository, and it is currently not mounted to a host.
Mounted	A virtual copy has this status when it is mounted to a host. The virtual copy exist in both InServ Storage Server and the Recovery Manager repository.

6.15 Event Messages

If an error message is generated by Recovery Manager for Exchange while you are attempting to perform a particular operation, you can access a description of the event and possible remedies from the **About** menu tab.

- To open the event message document, select any tree node item the exception of the root node in the tree pane view, and click **About** > **Event Messages**.

  Once this menu option is selected, the event messages will be displayed through the default browser.

6.16 Analyzing the Repository

To analyze the repository for a particular storage group:

1. In the Virtual Copy node tree, right-click the name of the storage group you wish to analyze and then select **Analyze**.

   Result: The **Analyze Virtual Copy** dialog box appears,

2. Select the **Sync** checkbox if you want to sync the repository and the InServ.

3 Click **OK**.

Result: The virtual copies for the storage group will be analyzed and any out-of-sync virtual copies will be displayed.

6.17 Validating a Virtual Copy

A mounted virtual copy can be validated with Exchange APIs through Recovery Manager.

- To validate an existing mounted Virtual Copy for a particular storage group, in the node tree, right-click the timestamp under the Storage Group virtual copy you wish to mount and then select **Validate**.

  Result: The virtual copy for the storage group will be validated.

7 Using the Recovery Manager CLI

In this chapter

7.1 Recovery Manager for Exchange Command Line Interface (CLI) 7.2

7.2 Recovery Manager Commands 7.3

RMExch analyze 7.4

RMExch backup 7.5

RMExch config 7.7

RMExch create 7.8

RMExch deletebackup 7.11

RMExch display 7.12

RMExch listbackup 7.14

RMExch mount 7.15

RMExch peer 7.17

RMExch policy 7.18

RMExch portconfig 7.20

RMExch rcstatus 7.21

RMExch remove 7.23

RMExch report 7.24

RMExch repository 7.25

RMExch reset 7.26

RMExch restore 7.28

RMExch unmount 7.32

RMExch validate 7.34

7.3 Running Recovery Manager as a Scheduled Job 7.35

7.1 Recovery Manager for Exchange Command Line Interface (CLI)

The Recovery Manager provides a CLI (Command Line Interface) that allows you to perform the following:

- Create virtual copies
- Remove virtual copies
- Validate virtual mounted copies with the eseutil.exe tool
- Reset mounting status in a repository or release operation lock status
- Compare current repository list for the specified storage group with the virtual copies on an InServ to detect any out-of-sync snapshots
- Mount virtual copies
- Unmount virtual copies
- Back up virtual copies to media using Symantec NetBackup
- Restore backed up virtual copies using Symantec NetBackup
- Configure the peer backup server for CCR configurations
- List available backups to restore from
- Delete a backup entry from the repository
  (**Note:** This does not remove the backup entry from NetBackup)
- Restore a storage group through filecopy from a mounted virtual copy

- Restore a storage group through volume restore from an unmounted virtual copy
- Display virtual copies currently in the repository and their status
- Set/Display maximum number of virtual copies to maintain
- Set/Display Recovery Manager communication port
- Set/Display advanced configuration for backup timeout and remote copy monitoring interval
- Set/Display remote copy history
- Gather system configuration for troubleshooting purposes

The following sections describe how to administer Recovery Manager from the Command Line Interface.

7.2 Recovery Manager Commands

This section describes the commands that can be run from the Command Line Interface:

COMMAND

`RMExch analyze`

SYNTAX

```
RMExch analyze -s <ExchangeServer> -g <StorageGroup> [-sync] [-f]
[-InServ <InServID>]
```

DESCRIPTION

The `RMExch analyze` command analyzes the existing repository and lists any out-of-sync virtual copies information between the repository and InServ.

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - The name of the exchange server for which the storage group belongs.
- `-g <StorageGroup>` - The name of the storage group for which the virtual copy timestamp belongs.



NOTE: Use quotes ("") for names that include spaces.

- `-sync` - Automatically updates the repository to match InServ information. If a virtual copy is missing virtual volumes, it is removed from the repository.
- `-f` - Forces the command. This option can only be used if the `-sync` option is used.
- `-InServ <InServID>` - Specifies the InServ to analyze if the backup server is configured for more than one InServ. If not specified, the default InServ detected is used.

EXAMPLES

The following commands will analyze existing repository and output any out-of-sync information.

```
RMExch analyze -s bottlenosed -g sg2
RMExch analyze -s bottlenosed -g "First storage group"
```

COMMAND

`RMExch backup`

SYNTAX

```
RMExch backup -s <ExchangeServer> -g <storagegroup>
[-t <Timestamp>] -p <policyName> [-remove]
-d <fullScheduleName> -m <masterServer> [-defer|-nc]
[-mp <"mountpoint">] [-active][-passive][-lcr]
```

DESCRIPTION

The `RMExch backup` command backs up a virtual copy to media, or creates a virtual copy and backs up to media (also known as a quick backup). For the latter case, no timestamp is needed.

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - The name of the exchange server for which the storage group belongs.
- `-g <Storage_group>` - The name of the storage group for which the timestamp belongs.
- `–t <Timestamp>` - This is optional. The timestamp of the virtual copy to backup. Use if the virtual copy has already been created. Do not use to create a virtual copy and then perform a backup.
- `–p <policyName>` - Name of the NBU policy set up for virtual copy DBA.
- `-remove` - This is optional and used with quick backups. Specify this option to remove the virtual copy after a quick backup. By default the virtual copy will be retained.
- `–d <fullScheduleName>` - Name of NBU full schedule set up for virtual copy DBA.
- `–m <masterServer>` - Name of the NBU master server.
- `-defer` - This is optional. To defer the Exchange log truncation after the successful backup is confirmed in automatic creation. This option is to defer log truncation until backup completion, keeping the Exchange writer in "waiting for completion" state that period. This option cannot be used with the `-t` option.

- `-nc` - This is optional. Skips the integrity check (not recommended). This option cannot be used with the `-t` or `-defer` options.



NOTE: The `-defer` option is not supported when the Recovery Manager for Exchange backup server is the same as the production server.

- `-mp "mountpoint"` - This is optional. Specifies the mount point (delimited by quotation marks), for a backup location other than in the default directory.
  - Full path is required.
  - Default is `<System Drive>:\3parsnapshot`.
  - If the specified virtual copy is already mounted, this parameter will be ignored.
- `-lcr` - Optional - Take the snapshot from the local continuous replication copy.
- `-active` - Optional - One step backup from the active CCR node (applies for CCR configurations only, and can only backup for the node at the local site). The active node is the default if `-active` is not specified.
- `-passive` - Optional - One step backup on the passive CCR node (applies for CCR configurations only, and can only backup for the node at the local site). The active node is the default if `-passive` or `-active` are not specified.



NOTE: Use quotes ("") where spaces are included.



NOTE: Symantec NetBackup software is case sensitive. Make sure all information entered pertaining to the policy is supplied with the proper case.

EXAMPLE

The following command will perform a backup of virtual copy 020405162103 whose data has currently been mounted.

```
RMExch backup -s bottlenosed -g sg2 -t 020405162103 -p test -d full -m
bottlenosed
```

COMMAND

`RMExch config`

SYNTAX

To change/query the timeout value for NetBackup initialization process detection:

```
RMExch config -h <WindowsHost> -bktmout [-sec <seconds>]
```

To change/query the monitoring interval for remote copy progress on target server:

```
RMExch config -h <WindowsHost> -rcintvl [-min <Minutes>]
```

DESCRIPTION

The `RMExch config` command will display or change the timeout value for NetBackup initialization process detection for backup operation and the monitoring interval for remote copy progress on target server.

PARAMETERS

The following options are supported:

- `-h <WindowsHost>` - Specify the Recovery Manager installed Windows host to change or query settings.
- `-bktmout` - Setup or inquiry for Backup process timeout value to confirm that NetBackup has received the backup request. Default is 30 seconds.
- `-min <Minutes>` - This is optional. Specifies the number of minutes.
- `-sec <Seconds>` - This is optional. Specifies the number of seconds. This option can only be used if the `-bktmout` option is also specified.
- `-rcintvl` - Setup or inquery for Remote Copy process monitoring interval. Default is 3 minutes.

EXAMPLE

The following command will change Remote Copy monitoring interval to 10 minutes.

```
RMExch config -h Grampus -rcintvl -min 10
```

COMMAND

`RMExch create`

SYNTAX

```
RMExch create -s <ExchangeServer> -g <StorageGroup> [-nc [-truncate]]
[-rc <TargetServer> [-defer]] [-active] [-passive] [-both] [-lcr]
```

DESCRIPTION

The `RMExch create` command creates a virtual copy of a storage group on the primary host where Exchange is running. As part of virtual copy create process, virtual copy will be exposed to the backup host for data integrity checking as default options. Once virtual copy validated successfully, the Exchange transaction log will be truncated as default setting.

- This command only supports online backup of an entire storage group; therefore, you must make sure the storage group is online before continuing with the virtual copy creation.

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - Exchange server for which storage group belongs. This parameter is case sensitive.
- `-g <StorageGroup>` - The storage group to shadow copy. This parameter is case sensitive.
- `-nc` - Optional - Skip the integrity check. Not recommended.
- `-truncate` - Optional - Force truncation of log upon successful VC creation when -nc is used.
- `-rc <TargetServer>` - Optional - Indicates the virtual copy creation is for remote copy. Specify target server to create virtual copy once remote copy completes.
- `-defer` - Optional - Defer the log truncation decision after the Remote Copy completes. This option is to defer log truncation until backup completion, keeping the Exchange writer in "waiting for completion" state that period.
- `-lcr` - Optional - Take the snapshot from the local continuous replication copy.
- `-active` - Optional - Take the snapshot from the active CCR node (applies for CCR configurations only). The active node is the default if -active is not specified

- `-passive` - Optional - Take the snapshot on the passive CCR node (applies for CCR configurations only). The active node is the default if -passive or -active are not specified.
- `-both` - Optional - Take the snapshot on both active and passive nodes.



NOTE: Use quotes ("") for names that include spaces.



NOTE: The command will attempt to take a snapshot on the passive node first then take a snapshot on active node after if the `-both` option is specified during the CCR configuration. A success status indicates at least one of the snapshot creations was successful.

EXAMPLES

The following command will create a snapshot for the storage group sg2 on exchange server bottlenosed.

```
RMExch create -s bottlenosed -g sg2
```

The following command will create a snapshot for the storage group sg2 on exchange server bottlenosed off the locally replicated copy.

```
RMExch create -s bottlenosed -g sg2 -lcr
```



NOTE: The target server to create snapshots upon the completion of remote copy process has to have the same version of Recovery Manager Backup Server component installed. Refer to Remote Copy Integration for more information on the Remote Copy setup.



NOTE: It is the user's responsibility to perform data integrity checking and transaction log truncation to the virtual copy created with the "-nc" option. Skipping data integrity checking is not recommend.



NOTE: VSS will wait for up to 10 seconds for the writers to freeze I/O, and this interval is not configurable. In most cases 10 seconds is a sufficient window to successfully create a virtual copy. However, in some circumstances under very heavy load, 10 seconds may not be enough and the virtual copy will fail on this attempt, which is "by design". VSS does not automatically retry the shadow copy creation, you must retry the virtual copy creation using the Recovery Manager GUI or the command line.



NOTE: During virtual copy creation, Recovery Manager dismounts and unmasks the virtual copy device from the Windows server, and breaks the virtual copy away from VSS control. During this process a "delayed write error" message may show up, or the message "the system failed to flush data to the transaction log" may appear in the System Event Log. This is normal.

COMMAND

`RMExch deletebackup`

SYNTAX

```
RMExch deletebackup -s <ExchangeServer> -g <storagegroup>
-t <backuptimestamp>
```

DESCRIPTION

The `RMExch deletebackup` command removes a backup entry in the backup repository. It will not communicate to Netbackup to delete the actual backup.

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - The name of the exchange server for which the storage group belongs.
- `-g <StorageGroup>` - The name of the storage group of the virtual copy that was backed up to belongs.
- `-t <BackupTimestamp>` - The timestamp of the virtual copy that was backed up.



NOTE: Use quotes ("") where spaces are included.

EXAMPLE

The following command will delete a backup with the timestamp 020405162103

```
RMExch deletebackup -s bottlenosed -g sg2 -t 020405162103
```

COMMAND

`RMExch display`

SYNTAX

```
RMExch display <-s Exchangeserver> <-g storagegroup> [-h WindowsHost]
[-t timestamp] [-inserv InservId]
```

DESCRIPTION

The `RMExch display` command displays all virtual copies in the repository.

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - The name of the exchange server for which the storage group belongs. If this is not given then the machine name will be used.
- `-g <StorageGroup>` - The name of the storage group for which the virtual copy information is to be retrieved.
- `-h <WindowsHost>` - This is optional. Specifies a Recovery Manager installed Windows host to query repository information.
- `-t <timestamp>` - This is optional. Specify a timestamp to display more detail for that virtual copy.
- `-inserv <InservId>` - This is optional. Inserv System Identifier.



NOTE: Use quotes (" ") where spaces are included.



NOTE: If a storage group name is given, the Exchange Server name must also be provided. If both the Exchange Server and storage group names are not given, then the Exchange Server defaults to the machine name.

EXAMPLES

The following commands will display the virtual copies for Exchange server Alpha and storage group Zeta.

```
RMExch display -s Alpha -g Zeta
RMExch display -s xexchange -g ssg2 -inserv 418
```


3PAR Confidential

COMMAND

`RMExch listbackup`

SYNTAX

```
RMExch listbackup -s <ExchangeServer> [-bs Backup Server]
```

DESCRIPTION

The `RMExch listbackup` command prints a list of the virtual copies backups that have been backed up by RMExch backup. For CCR configurations, different backups are listed on each backup server. Use the -bs parameter to list the backups for the backup server you are interested in.

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - The name of the exchange server for which the storage group belongs.
- `-bs <Backup Server>` - For CCR configurations only. List the backups maintained on the target backup server.

EXAMPLE

The following command will list the backups performed through Recovery Manager for host bottlenosed.

```
RMExch listbackup -s bottlenosed
```

COMMAND

`RMExch mount`

SYNTAX

```
RMExch mount -s <ExchangeServer> -g <StorageGroup> -t <Timestamp>
-h <Hostname> [-mp "mountpoint"] | <-expose InServHost>
```

DESCRIPTION

The `RMExch mount` command mounts a virtual copy created by the `RMExch create` command. When performing a `RMExch mount` to mount a virtual copy, the program will check to see if the virtual copy is already mounted to a host machine. The virtual copy must have an "Available" status, before it can be mounted

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - The name of the exchange server for which the storage group belongs.
- `-g <StorageGroup>` - The name of the storage group for which the virtual copy timestamp belongs.
- `-t <Timestamp>` - The timestamp of the virtual copy to mount.
- `-h <host>` - Windows host name to mount the virtual copy. The target host must have recovery manager installed.
- `-expose <InServHost>` - This is required if the `-h` option is not used. Specify this argument to expose virtual copy to the volume manager of the target system without assigning a mount point. This cannot be used in conjunction with the `-h` argument. The target host does not need to have Recovery Manager installed. This option is deprecated and will be removed in a future release.
- `-mp "mountpoint"` Optional - Quotation enclosed mount point, if you prefer to mount the volume(s) elsewhere besides default directory. Full path is required. Default is to mount to `<System Drive>:\3parsnapshot.`



NOTE: Use quotes ("") where spaces are included.



NOTE: The <InServHost> is the host name defined in the InServ Storage system. Available host name defined in InServ Storage system can be listed by executing the Inform CLI `showhost` command.



NOTE: The `-expose` host name is case-sensitive and must be the same as how it is defined on the InServ storage server.

EXAMPLES

The following command will mount the virtual copy 020405162103 to the directory d:\Rmmount.

```
RMExch mount -s bottlenosed -g sg2 -t 020405162103 -h bottlenosed -mp
"d:\RMmount"
```

COMMAND

`RMExch peer`

SYNTAX

```
RMExch peer [[<display>]|[-clear]|[-bs <peer_server>]]
```

DESCRIPTION

The `RMExch peer` command configures the peer backup servers for two InServ CCR configurations. The backup server executes all commands and sends certain commands to the peer backup server to run (such as create and backup) for the passive node option. Once the configuration is set, you will not need to run this command again unless you want to change the peer relationship between the backup servers.

PARAMETERS

The following options are supported:

- `-bs <peer_server>` - The server's name you would like to designate as your peer backup server.
- `-display` - Used if the `-bs` parameter is not used. Displays the current configuration of your peer backup servers.
- `-clear` - To remove the peer relationship between backup servers. Once the peer relationship is removed, both backup servers are no long able to manage CCR nodes.



NOTE: The `RMExch peer` command is intended only for CCR configuration. The `-bs` option only needs to be run once to set up the peer relationship and to manage the CCR configuration.

EXAMPLES

The following command will configure the peer backup server `server1`.

```
RMExch peer -bs server1
```

COMMAND

`RMExch policy`

SYNTAX

```
RMExch policy -s <ExchangeServer> -g <StorageGroup> -i <MaxVCAllowed>
[-r]
```

DESCRIPTION

The `RMExch policy` command will display or update the policy for the specified Exchange server. When only the `-s` argument is supplied, this command will list the current policy for the specified Exchange server. When `-i` is supplied, the policy will be updated to the argument followed by `-i`. If the optional `-r` argument is supplied, Recovery Manager will automatically remove the oldest virtual copy if the maximum number is exceeded. If it is not supplied, Recovery Manager will not automatically remove the oldest virtual copy when the maximum number is exceeded. The maximum value allowed for policy setting is 500.

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - The name of the Exchange server to display/update the policy configuration.
- `-g <StorageGroup>` - The name of the storage group.
- `-i <MaxVCAllowed>` - This is optional. Set the maximum number of virtual copies allowed for every storage group under the specified server.
- `-r` - This is optional. If specified, Recovery Manager will remove the oldest virtual copy once the maximum number of virtual copies has been created. If not specified, the oldest virtual copy is retained.



NOTE: Use quotes (" ") where spaces are included.

EXAMPLES

The following command will display current number of virtual copies allowed for any storage group under the specified server.

```
RMExch policy -s bottlenosed -g storageGroup
```

The following command will change the maximum virtual copies allowed for any storage group under bottlenosed to 10 and remove the oldest virtual copy when the maximum number is reached.

```
RMExch policy -s bottlenosed -g "first storage group" -i 10 -r
```

COMMAND

RMExch portconfig

SYNTAX

```
RMExch portconfig -h <WindowsServer> [-p <portnumber>]
```

DESCRIPTION

The RMExch portconfig command will display or update the current port configuration for the Recovery Manager service and RMExch CLI for the specified windows server. When only the -h argument is supplied, this command will list the current port number used by Recovery Manager for the Windows server. When -p is supplied, the port will be updated to the argument followed by -p. The default port used by Recovery Manager is 9933. This should be run against all of the production servers and backup servers. If you update the port setting on a windows server, you will need to restart the Recovery Manager for Exchange Agent Service before connecting through that port.

PARAMETERS

The following options are supported:

- -h <WindowsServer> - The name of the windows server to display/update the port configuration.
- -p <portnumber> - This is optional. If specified, the command will update the port used. If unspecified, the command will show the current configuration.

EXAMPLES

The following command will display the current port configuration for server Alpha.

```
RMExch portconfig -h Alpha
```

The following command will update the port configuration for server Alpha to 9950.

```
RMExch portconfig -h Alpha -p 9950
```

COMMAND

`RMExch rcstatus`

SYNTAX

```
RMExch rcstatus -s <ExchangeServer> -g <StorageGroup> <[-query]|[<-
update> [-t <timestamp> -ts <RecordKeeper> -status <RCStatus>]]>
```

DESCRIPTION

The `RMExch rcstatus` command will display or update status of the remote copy operation history.

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - Exchange server for which storage group belongs.
- `-g <StorageGroup>` - The storage group of the virtual copy.
- `-update` - Update the status of RC history for a specific timestamp.
- `-query` - Query RC history for specified storage group.
- `-t <Timestamp>` - The timestamp of the virtual copy.
- `-ts <Record Keeper>` - The target host to update the RC status record.
- `-status` - The status to save in record.



NOTE: The -update option without timestamp and host will update all RC records from the original target server.



NOTE: Use quotes (" ") where spaces are included.

EXAMPLES

The following command updates the status of an existing rcstatus history for the specified host.

```
RMExch rcstatus -s bottlenosed -g sg2 -t 050106113456 -ts Grampus -status
Success
```

The following command will update the existing rcstatus history in specified host by re-querying information from target server.

```
RMExch rcstatus -s bottlenosed -g "First storage group" -update -t 050106113456
-ts Grampus -status Success
```

COMMAND

`RMExch remove`

SYNTAX

```
RMExch remove -s <ExchangeServer> -g <StorageGroup> -t <Timestamp>
```

DESCRIPTION

The `RMExch remove` command removes the virtual copy from the InServ Storage Server and the repository. The virtual copy must have an "Available" status; if the virtual copy is mounted it will not be removed.

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - The name of the exchange server to which the storage group belongs.
- `-g <StorageGroup>` - The name of the storage group to which the virtual copy timestamp belongs.
- `–t <Timestamp>` - The timestamp of the virtual copy to remove.



NOTE: Use quotes ("") for names that include spaces.

EXAMPLE

The following command will remove the virtual copy with timestamp 020405162103.

```
RMExch remove -s bottlenosed -g sg2 -t 020405162103
```

COMMAND

`RMExch report`

SYNTAX

```
RMExch report -h <WindowsHost> -output <OutputDirectory>
```

DESCRIPTION

The `RMExch report` command will execute the RMReport batch script under the <InstallationPath>\Exchange\goodies folder and gather needed information on the specified Windows host for troubleshooting purposes.

PARAMETERS

The following options are supported:

- `-h <WindowHost>` - Specify a Recovery Manager installed Windows host to run RMREPORT utility.
- `-output <OutputFolder>` - The full path folder to receive the generated report.



NOTE: Use quotes ("") where spaces are included.

EXAMPLE

The following command will collect remote information related to RM activities.

```
RMExch report -h Grampus -output c:\MyReport
```

COMMAND

`RMExch repository`

SYNTAX

```
RMExch repository [-a <newRepositoryLocation>]
```

DESCRIPTION

The `RMExch repository` command will display or move the current repository locations for Recovery Manager. If no arguments are specified, then the current location is displayed. If `-a` is specified along with a directory, then the repository will be moved to the new location.

PARAMETERS

The following options are supported:

- `-a <newRepositorylocation>` - The target directory to move the repository to.

EXAMPLE

The following command will change the repository location to "e:\3PAR Storage"

```
RMExch repository -a "e:\3PAR Storage"
```


3PAR Confidential

COMMAND

`RMExch reset`

SYNTAX

To reset the Recovery Manager locking on remote Windows host:

```
RMExch reset <-s exchange server> <-opt lock>
```

To reset the mount status of a particular timestamp record:

```
RMExch reset <-s exchange server> <-g storage group>
<-t timestamp> <-opt status>
```

DESCRIPTION

The `RMExch reset` command resets a virtual copy mounting status in the repository record and internal process locking status on any designated Recovery Manager for Exchange installed system with only the "status" option being supported. Executing this command with 'status' option will force the removal of currently exposed VLUNs and set the mounting status to "Available".

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - The name of the exchange server for which the storage group belongs.
- `-g <StorageGroup>` - The name of the storage group for which the virtual copy timestamp belongs.
- `–t <Timestamp>` - Optional - The timestamp of the virtual copy. Requires <-opt status> option.
- `-opt <Option>` - Specifies whether to reset the locking or mounting status. Currently supported options are 'lock' and 'status'. The 'lock' option is only used to unlock Recovery Manager from previous VC creation failure caused by unexpected termination.



NOTE: Reset status of a specific timestamp will force the removal of currently exposed VLUNs.



NOTE: Use quotes ("") for names that include spaces.



NOTE: When Recovery Manager is processing user requests, it will activate an internal locking mechanism. Any incoming request will get "Server <ServerName> has a Recovery Manager command running already" message. Please wait until it finishes before continuing. However, in the case of unexpected termination, the locking status might not get deactivated properly. You need to use this command to release the lock for the operation to go back to normal status.

EXAMPLES

The following commands will reset the existing mount status to available.

```
RMExch reset -s bottlenosed -g sg2 -t 050106113456 -opt status

RMExch reset -s bottlenosed -g "First storage group" -t 050106113456 -opt
status
```


3PAR Confidential

COMMAND

RMExch restore

SYNTAX

For MEDIA RESTORES

```
RMExch restore -s <ExchangeServer> -g <storagegroup> -t <Timestamp> -p
<policyName> -m <masterServer> [-a <altLocation>] [-src
<OrignalClientWithBackups>]
```

For FILECOPY and VOLUME RESTORES

```
RMExch restore -s <ExchangeServer> -g <storagegroup> -t <Timestamp>
<-filecopy | -promote>
```

DESCRIPTION

The RMExch restore command can perform one of three functions. It can restore a previously backed up virtual copy from media, perform a filecopy restore from a mounted virtual copy, or perform a volume restore from an unmounted virtual copy.

Media backups can be restored to their original location (the volume(s) or directory locations of the virtual copies that were backed up. Note: not original exchange data locations, or an alternate location can be specified.

Filecopy restores will copy the virtual copy's files to the original database location and overwrite the current database files. The virtual copy to be restored from must be mounted to the production server hosting the storage group. See Chapter 8 *Recovery Procedures* on page 8.4.

Volume promote restores will overwrite all data on the original database volume. This will overwrite ALL data on the original volume and should only be performed with this understanding. See Chapter 8 *Recovery Procedures* on page 8.4.



WARNING: Please DO NOT perform a volume promote restore if multiple storage groups share any volumes. This includes all data files .LOG, .EDB, .CHK (and .STM for Exchange 2003). If you are not sure how or if your storage groups share volumes, please execute the script "chk_multi_storage.cmd" by default installed at "Program Files/3PAR/RM/Exchange/bin/" to determine how any storage groups may be sharing volumes.

PARAMETERS

For MEDIA RESTORES

The following options are supported:

- `-s <ExchangeServer>` - The name of the exchange server for which the storage group belongs.
- `-g <storagegroup>` - The name of the storage group for which the timestamp belongs.
- `-t <Timestamp>` - The timestamp of the virtual copy to restore.
- `-p <policyName>` - Name of the NBU policy set up for Recovery Manager.
- `-m <masterServer>` - Name of the NBU master server.
- `-a <altLocation>` - This is optional. Alternate restore location.
- `-src <OrignalClientWithBackups>` - This is optional. Specifies the client name to use for finding backups or archives from which to restore files. The default is the current client name.



NOTE: Use quotes ("") where spaces are included.



NOTE: If the restore is directed to the original location, ensure the original location is still valid.



NOTE: Symantec NetBackup software is case sensitive. Make sure all information entered pertaining to the policy is with the exact case.



NOTE: Make sure the Symantec NetBackup software's bin directory is in the system search path for this command to run.



NOTE: When a volume promote is executed on a passive node in a CCR setup, the `RMExch restore` command usage will be displayed if the CCR nodes are managed by single backup server. Otherwise, a proper error message is displayed.

EXAMPLE

The following command will perform a restore of a virtual copy 020405162103 from Netbackup media to drive J:\.

```
RMExch restore -s bottlenosed -g sg2 -t 020405162103 -p test -m bottlenosed -a
J:\
```

PARAMETERS

For FILECOPY and VOLUME RESTORES

The following options are supported:

`-s <ExchangeServer>` - The name of the exchange server for which the storage group belongs.

`-g <storagegroup>` - The name of the storage group for which the timestamp belongs.

`-t <Timestamp>` - The timestamp of the virtual copy to restore.

`<-filecopy | -promote>` - Specify whether you'd like to perform a filecopy restore or a volume promote restore.



NOTE: Use quotes (" ") where spaces are included.

EXAMPLES

The following command will perform a restore of a virtual copy with the timestamp020405162103 to original database location:

```
RMExch restore -s bottlenosed -g sg2 -t 020405162103 -filecopy
```

The following command will perform a volume restore of an unmounted virtual copy with the timestamp 020405162103 to the original database volumes:

```
RMExch restore -s bottlenosed -g sg2 -t 020405162103 -promote
```


3PAR Confidential

COMMAND

`RMExch unmount`

SYNTAX

```
RMExch unmount -s <ExchangeServer> -g <StorageGroup> -t <Timestamp>
-h <hostname>
```

DESCRIPTION

The `RMExch unmount` command unmounts a currently mounted virtual copy. When performing `RMExch mount` to mount a virtual copy, the program will check to see if the virtual copy is mounted to a host machine. The virtual copy must have a status of "Mounted" or "Exposed" before it can be unmounted.

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - The name of the exchange server for which the storage group belongs.
- `-g <StorageGroup>` - The name of the storage group for which the virtual copy timestamp belongs.
- `-t <Timestamp>` - The timestamp of the virtual copy to unmount.
- `-h <hostname>` - This is optional. The windows hostname (other than the default host) for the host to unmount the virtual copy from. Host has to have Recovery Manager installed. This option is deprecated and will be removed in a future release.



NOTE: Unmount the exposed volume, specify the local Windows host name in -h option.



NOTE: Use quotes ("") where spaces are included.

EXAMPLES

The following command will unmount the virtual copy 020405162103.

```
RMExch unmount -s bottlenosed -g sg2 -t 020405162103 -h bottlenosed
```

COMMAND

`RMExch validate`

SYNTAX

```
RMExch validate -s <ExchangeServer> -g <StorageGroup>
-t <Timestamp>
```

DESCRIPTION

The `RMExch validate` command verifies the data integrity of the exchange database files in the specified virtual copy that is already mounted on the system.

PARAMETERS

The following options are supported:

- `-s <ExchangeServer>` - The name of the exchange server for which the storage group belongs.
- `-g <StorageGroup>` - The name of the storage group for which the virtual copy timestamp belongs.
- `–t <Timestamp>` - The already mounted timestamp for validation.



NOTE: Use quotes (" ") for names that include spaces.



WARNING: If the validation operation failed on the virtual copy, the failed virtual copy cannot be used for backup and restoration purposes. It is the user's responsibility to manually remove the failed virtual copy.

EXAMPLE

The following command validates the specified exchange database.

```
RMExch validate -s bottlenosed -g sg2 -t 020405162103
```

7.3 Running Recovery Manager as a Scheduled Job

In addition to creating virtual copies using the command line, you can also schedule virtual copies to be created for a specific storage group using Windows Scheduled Tasks.



NOTE: The following instructions are for Windows 2003 and may differ in some places for later versions.

To create virtual copies using Windows Scheduled Tasks:

1. Click **Start** > **Programs** > **Accessories** > **System Tools** > **Scheduled Tasks**.

   Result: The **Scheduled Tasks** window appears.

2. Double-click **Add Scheduled Tasks**.

   Result: The **Scheduled Task Wizard** appears.

3. Click **Next** to continue.

4. Click **Browse** and navigate to the Recovery Manager install location. The default location is `C:/Program Files/3PAR/RM/Exchange/bin.`

5. Click **RMExch.exe** and then select the frequency of this task.

6. Click **Next** to continue.

7. Select the start time, frequency, and start date for the task, and then click **Next**.

8. Enter the user name, password, and password confirmation, and then click **Next**.



NOTE: Since the command `RMExch create` communicates with Exchange via the file `CDOEXM.dll`, access privilege should be granted to a user such as Exchange administrator.

9. Select the **Open advanced properties...** checkbox, and click **Finish** to access advanced setup for the scheduled task. \

   Result: The **RMexch** window appears.

10 On the **Task** tab, at the end of the path displayed in the **Run** field, add `-s <exchange server name> -g <storage group name>`. If the storage group name has spaces, use double-quotes "`text`" around the name.

For example:

```
From -> C:\Program Files\3par\RM\Exchange\bin\
Type -> RMExch create -s MyExchangeServ -g "First storage group"
```



NOTE: On Windows 2008, the RMexch options should specified through the "Add arguments (optional)" box. For example:

Program/Script: `C:\Program Files\3par\RM\Exchange\bin\RMexch.exe`

Add arguments (optional): `create -s MyExchangeServer -g "First Storage Group"`

11 On the **Schedule** tab, further refine the scheduled task by selecting the frequency and start time of the task.

12 Click **Apply** and then **OK** when finished.

Result: Virtual copies are created as you have scheduled. Depending on the policy set with the Recovery Manager GUI, older virtual copies on the system may automatically be removed if the number of virtual copies exceeds your specified maximum threshold (see *Setting Recovery Manager Policy Configuration* on page 6.6).

8 Rapid Backup and Recovery for Exchange

In this chapter

8.1 Key Microsoft Exchange File Types 8.2

8.2 Backup 8.3

8.3 Virtual Copies 8.3

8.3.1 Advantages of Using Recovery Manager 8.3

8.4 Recovery Procedures 8.4

8.4.1 Point-In-Time Recovery 8.4

8.4.2 Volume Promote Point-In-Time Recovery 8.6

8.4.3 Point-Of-Failure Recovery 8.8

8.4.4 Single Mailbox Recovery 8.9

8.4.5 Using the Recovery Storage Group Feature 8.13

8.5 Additional Documentation 8.17

3PAR Confidential

8.1 Key Microsoft Exchange File Types

Before discussing backup and recovery for Microsoft Exchange, it is important to understand the elements of Exchange.

Microsoft Exchange uses five key file types for all operations:

- Log file (*.LOG). A 5 MB file in which transaction log records are stored.
- Patch file (*.PAT). Used during backup, restore, and recovery operations, it contains database pages that were split during online backup.
- Checkpoint file (*.CHK). Maintains information about the location in the transaction logs that was last committed to the database.
- Database file (*.EDB). Properties data file to store all user data.

There are three key files within Microsoft Exchange storage groups: EDB, CHK, and LOG files. LOG files are accessed in a sequential order; EDB files are accessed with random I/O patterns. For optimal performance and to facilitate database management, transaction logs should be placed on a volume that performs sequential I/O in an optimal manner such as a RAID 1 volume. The EDB files should be placed on a separate volume that is optimized for random I/O such as a RAID 5 volume. For additional information on creating volumes, see the *3PAR InForm OS CLI Administrator's Manual*.

From the performance and management point of view, a dedicated volume should be created for every log file group on each storage group and another data volume should be created for combined EDB files for each data store on every storage group. For example, if you have two storage groups, each with a log and five mailbox stores, create two RAID 1 volumes for the logs and ten RAID 5 volumes for the EDB files.

When a change is made to the Exchange database, Exchange updates the data in the memory (4K pages) and synchronously writes a record of the transaction to the log in sequential order. This record allows Exchange to re-create the transaction in the event of a failure. The database engine then writes the data to the disk in large I/O operations. Exchange supports *circular logging* to save disk space on the volume containing log files. However, circular logging makes hard recovery (restoring from backup) impossible. It is recommended that the circular logging feature be disabled. Circular logging is disabled by default from Microsoft Exchange.

8.2 Backup

An online backup of Exchange runs while the data store is mounted. A full backup backs up the entire information store and transaction log. It also truncates the log after the log has been backed up to reduce disk space usage.

8.3 Virtual Copies

A virtual copy is a copy of another virtual volume (EDB or LOG) created using copy-on-write techniques. Unlike a physical copy, which is a duplicate of the entire virtual volume, a virtual copy, or snapshot, only records the changes to the original virtual volume. Therefore, minimal storage space is used. This allows an earlier state of the original virtual volume to be recreated by starting with its current state and rolling back all the changes that have been made since the virtual copy was created. The system allows you to make up to 500 virtual copies of each virtual volume, assuming that sufficient storage space was allocated when the base virtual volume was created.

8.3.1 Advantages of Using Recovery Manager

Traditionally, databases are backed up to tape. Backing up to tape is a time consuming task, especially if the database is growing rapidly. Recovery Manager offers the following advantages over traditional tape backup:

- Creating virtual copies of databases using Recovery Manager requires only seconds and can be accomplished via the click of the mouse through the Recovery Manager GUI, or by even scheduling virtual copies via Windows' automatic scheduled task application. For details on using the GUI and scheduling tasks in Windows, see *Creating a Virtual Copy* on page 6.7 and *RMExch create* on page 7.8, respectively.
- With Recovery Manager's optional policy settings, you can maintain a specified number of the latest virtual copies to stay online. These online virtual copies can then be mounted to the staging Exchange server for point-in-time recovery, thus eliminating the need to restore from tape, which can take hours.
- After the virtual copy has been mounted to the backup server, you can then perform a backup to tape of the virtual copy using Recovery Manager.
- Easy recovery through filecopy and volume promote restores.



NOTE: Backup to tape can be performed in one easy command with a quick backup. See *RMExch backup* on page 7.5.

8.4 Recovery Procedures

In many cases, the Exchange server is able to quietly recover when a server crashes and the contents of the database buffer in the memory are lost. Exchange automatically recovers when you start the information store after the failure using the checkpoint file to identify the oldest transaction not flushed to disk and then replaying log files forward. If the checkpoint file is missing, all the log files are scanned to determine if any committed transactions have not been written to the database. At the end, the database is consistent and can start normally. Most of the time, recovering an email or a user's email is all that is needed. This can be done by using the Recovery Storage Group.

Recovery Manager provides several options for a full storage group recovery if Recovery Storage Group is not sufficient:

- point-in-time recovery
- volume promote point-in-time recovery
- point-of-failure recovery
- single mailbox recovery

8.4.1 Point-In-Time Recovery

Recovery procedures for LCR or CCR Exchange 2007 configurations should be run on the active copy of the database (the active node for CCR). **Restores to the passive copy are not supported by Microsoft.** The passive copy will need to be reseeded after a restore is performed on the active copy.

To perform a point-in-time recovery:

1. In the **Exchange Management Console**, right-click the desired database you want to recover and select **Properties.**

   Result: The **Properties** dialog box appears.

2. Under the **General** tab, select **This database can be overwritten by a restore**.

3 Click **OK**.

4 On the **Database Management** tab in the **Exchange Management Console**, right-click the storage group you want to recover and select **Dismount Database**.



NOTE: If in a cluster, go to the **Cluster Administrator** and take the Exchange Information Store Instance resource offline. If not in a cluster, go to the services menu and stop the Exchange Information Store Service.

5 Mount the desired virtual copy to the staging Exchange server either from the Recovery Manager GUI or from the command line using the RMExch mount command. Refer to Chapter 6, *Using the Recovery Manager GUI* and Chapter 7, *Using the Recovery Manager CLI* for details on running Recovery Manager from the GUI and command line. If you are performing the restore in a CCR environment, suspend the replication using the **suspend-storagegroupcopy** command from the Exchange Management Shell. If you are performing the restore in a CCR environment, suspend the replication using the **suspend-storagegroupcopy** command from the Exchange Management Shell.

6 Delete the original .edb, .log, and .chk files for a clean restore. ONLY remove the files, NOT their parent/intermediate folders as the original database path and its structures must be kept the same. Also delete all catalog subdirectories under your database directories. You should also delete all catalog subdirectories under your database directories. The files may be moved to new locations instead of completely removed.

7 From the backup server, execute the Recovery Manager filecopy restore command: `rmexch restore -s <exchangeServer> -g <storageGroup> -t <timestamp> -filecopy`. You can alternately use the GUI to trigger a filecopy restore. Refer to Chapter 6 for detailed instructions on performing a filecopy restore.

8 After the filecopy restore completes and the database files are successfully recovered, the database can now be re-mounted to continue its operation. If performing the restore in a CCR environment, reseed the remote database using the **Update-StorageGroupCopy** command from the Exchange Management Shell. In some cases, you may need to use **Resume-StorageGroupCopy** to resume the replication. (Skip step 6 and beyond as those are the required steps for volume restore.)

9 If performing the restore in a CCR environment, reseed the remote database using the **Update-StorageGroupCopy** command from the Exchange Management Shell. Then use the **Resume-StorageGroupCopy** command to resume the replication.

8.4.2 Volume Promote Point-In-Time Recovery

To perform a volume promote point-in-time recovery, make sure the virtual copy you would like to promote has the status Available. If it is Mounted, unmount it. If you are not performing this restore in a Single Copy Cluster or a Continuous Copy Replication cluster, the steps involving cluster can be ignored.

For CCR environment volume promote restores, the following additional steps need to be performed:

1. Remove .edb, .log, and .chk files from both nodes. (Or move to a backup location).
2. Remove the catalog subdirectories in the .edb directories if they exist. Suspend the CCR.

For single copy cluster volume promote restores (not CCR), the following extra steps need to be performed:

1. All of the resources the storage group uses, including the disk(s) for the storage group's Log path, System path, and its mailbox(es)' database(s), need to be put in extended maintenance mode.
2. From the command line, issue the following command for all disks the storage group uses:

```
cluster res "resourcename" /maint:on
cluster res "resourcename" /waitmaint
```

3. From the **Cluster Administrator**, take the Disk(s) offline.
4. From the backup server, execute the Recovery Manager command for volume promote restore. For details refer to Chapter 7, *Using the Recovery Manager CLI* regarding information on executing the restore-promote command. Alternatively, refer to Chapter 6, *Using the Recovery Manager GUI*for information on using the GUI to execute a volume restore.



WARNING: DO NOT perform a volume promote restore if multiple storage groups share any volumes. This includes all data files .LOG, .EDB, .CHK (and .STM for Exchange 2003). If you are not sure how or if your storage groups share volumes, please execute the script "chk_multi_storage.cmd" by default installed at "Program Files/3PAR/RM/Exchange/bin" to determine how any storage groups may be sharing volumes.

5 In the **Computer Management** window, for volume promote restores, right-click the **Disk Management** node and select **Rescan Disks**.

6 From the **Cluster Administrator**, bring the Disk(s) back online.

7 Follow the appropriate steps depending on whether you are performing the operation for *Single Copy Clusters* or *Continuous Copy Replication Clusters*

8.4.2.1 Single Copy Clusters

1 For the disk(s) previously put in maintenance mode, take ALL of them out of maintenance mode.

2 From the command line, issue the following command for all disks the storage group uses:

```
Cluster res "resourcename" /maint:off
```

3 Verify the EDB, LOG, CHK files are correctly appearing in the original database locations.

4 Mount the databases within the storage group.

Result: The database is recovered to the point-in-time when the virtual copy was taken.

8.4.2.2 Continuous Copy Replication Clusters

1 Reseed the remote database using the command **Update-StorageGroupCopy** from the Exchange Management Shell.

2 Use **Resume-StorageGroupCopy** to resume the replication.



NOTE: For Exchange 2007 virtual copies created off the LCR copy, a volume promote restore is not supported.

8.4.3 Point-Of-Failure Recovery

This section provides instructions on performing a *Point-Of-Failure Recovery for Filecopy Restore* and performing a *Point-Of-Failure Recovery for Volume Restore*.

8.4.3.1 Point-Of-Failure Recovery for Filecopy Restore

To perform a point-of-failure recovery for filecopy restore:

1. Move the currently existing log files on your storage group volumes that you want to roll forward.



NOTE: If Windows will not allow you to move, or even copy, exchange .LOG files because "it is being used by another program," part of Exchange is still "live".If this is the case, move on to step 2

2. Repeat the point-in-time recovery for filecopy restore: step 1to step 4.
3. With Exchange database(s) dismounted, preserve the current log files on your Storage group volumes if you were not able to do so from step 1.
4. Mount the desired virtual copy for the staging Exchange server either from the Recovery Manager GUI or from the command line using the RMExch mount command. Refer to Chapter 6, *Using the Recovery Manager GUI* and Chapter 7, *Using the Recovery Manager CLI* for details on running Recovery Manager from the GUI and command line.
5. Delete the original .EDB, .LOG, and .CHK files for a clean restore. Please ONLY remove the files, NOT their parent/intermediate folders as the original database path and its structures must be kept the same. The files may be moved to new locations instead of completely removed.
6. Go to the backup server and execute the Recovery Manager filecopy restore command: `rmexch restore -s <exchangeServer> -g <storageGroup> -t <timestamp> -filecopy` (allternatively, you can execute a filecopy restore by using the GUI. See *File Copy Restore* on page 6.14).
7. Copy the .LOG files that you preserved (from steps 1 or 3) and overwrite the logs recovered. This includes the extra logs not covered by the virtual copy, making the recovery more forward-in-time.
8. Delete the checkpoint file. (.chk)
9. Now you are ready to re-mount the database(s) to continue.

Result: The Exchange server performs a soft recovery and automatically replays the log. Once the store is mounted, a confirmation is displayed.



NOTE: In some situations Exchange may display a warning message indicating one or more log(s) are out of sync. In such cases no confirmation is displayed. For Exchange 2007, usually no confirmation is displayed.

8.4.3.2 Point-Of-Failure Recovery for Volume Restore

To perform a point-of-failure recovery for volume restore:

1. Move the currently existing log files on your storage group volumes that you want to roll forward.



NOTE: If Windows will allow you to move, or even copy, exchange .LOG files because it is being used by another program, part of Exchange is still live. If this is the case, move on to step 2.

2. Repeat the point-in-time recovery for volume restore, step 1 on page 8.9to step 4 on page 8.8
3. With Exchange database(s) dismounted, preserve the current log files on your Storage group volumes if you were not able to do so from step 1 on page 8.9.
4. After you have put all the disk(s) out of maintenance mode, perform the following:
   a. Copy the .LOG files that you preserved and overwrite the logs recovered. This includes the extra logs not covered by the virtual copy, making the recovery more forward-in-time.
   b. Delete the checkpoint file (.CHK).
   c. Now you are ready to re-mount the database(s) to continue.

      Result: The Exchange server performs a soft recovery and automatically replays the log. Once the store is mounted, a confirmation is displayed.

8.4.4 Single Mailbox Recovery

There are several methods for single mailbox recovery with Exchange, this document will describe two methods:

- *Restoring a Mailbox from a Backup to a Recovery Server*
- *Using the Recovery Storage Group Feature*Using the Recovery Storage Group Feature

8.4.4.1 Restoring a Mailbox from a Backup to a Recovery Server

To restore a mailbox from backup, you must have a recovery server that has sufficient storage capacity to install Exchange Server and to restore the private information store database. This server can be on the same physical network as your production Exchange Server computer.

To restore a mailbox from a backup to a recovery server:

1. Take note of the following information that is on the production Exchange Server computer:
   - Organization Name
   - Administrative Group Name
   - Storage Group Name
2. On the recovery server, install the Windows Server operating system, and then create a new Active Directory forest.
3. Run the **Exchange Server Setup**, and create a new organization that uses the same name as your existing Exchange organization.
4. Do one of the following:
   a. If the name of your administrative group is *First Administrative Group*, go to step 6 on page 8.11.

      or:

   b. Install Exchange Server to an administrative group other than the *First Administrative Group*:

      1) Run Exchange Server Setup, and then install Microsoft Exchange System Management Tools.



NOTE: At this point, do not install Microsoft Exchange Messaging and Collaboration Services. Type the name of your administrative group (the same name as the administrative group on your production server).

      2) Start the **Exchange System Manager**.

3) Right-click your organization, and then click **Properties**.

4) Click the **General** tab, click to select the **Display administrative groups** check box, and then click **OK**.

5) Quit and then restart the **Exchange System Manager**.

6) Right-click **Administrative Groups**, point to **New**, and then click **Administrative Group**.

7) In the **Name** box, type the name of the administrative group, and then click **OK**.



NOTE: You must use the same name that you used to name the administrative group on your production Exchange Server computer.

8) Quit the **Exchange System Manager**.

5 Run the Exchange Server Setup and install Microsoft Exchange Messaging and Collaboration Service and Microsoft Exchange System Management Tools (if the Exchange System Management Tools are not already installed on the server).

6 Configure the storage group name to use the same name as the production Exchange Server computer.

a Start the **Exchange System Manager**.

b Expand **Administrative Groups**, and then expand **AdministrativeGroupName**.

c Expand **Servers** and then expand **YourServerName**.



NOTE: If the name of the storage group on the production server uses a name other than First Storage Group, configure the storage group name to use the same name as the storage group on the production Exchange Server computer.

7 Dismount the database:

a Right-click the **Mailbox Store** and click **Dismount Store**.

b Click **Yes** when you are prompted to continue.

c Right-click the **Mailbox Store** and select **Properties**.

d Select the **Database** tab and check the **This database can be overwritten by a restore** check box.

e Click **OK**.

f Quit the **Exchange System Manager**.

8 Delete the existing database and log files that are on the recovery server.

9 Restore the database files from backup.

10 To repair the database, run the following repair utility:

```
eseutil /r E0n /d<database file directory location> /l<log file
directory> /s<system file directory>
```

n should be replaced by the storage group number, e.g. E01, E02, E03.

11 Mount the database.

a Start the **Exchange System Manager.**

b Expand **Administrative Groups**, and then expand ***AdministrativeGroupName***.

c Expand **Servers**, expand ***YourServerName***, and then expand ***YourStorageGroupName***.

d Right-click the **Mailbox Store**, and click **Mount Store**.

e Click **OK** when you receive the message that indicates that the store successfully mounted.

12 Create a new user in **Active Directory Users and Computers**. Make sure that you do not make the new user account mailbox-enabled. To create the new user:

a Start **Active Directory Users and Computers**.

b Right-click **Users**, point to **New**, and then click **User**.

c Specify the user name and the user logon name in the appropriate boxes, and click **Next**.

d Specify the password information for the user, and click **Next**.

e Click to clear the **Create an Exchange mailbox** check box, and click **Next**.

f Click **Finish**.

13 In the **Exchange System Manager**, expand the **Mailbox Store**, right-click **Mailboxes**, and click **Run Cleanup Agent**.

14 Recover the mailbox.

a Right-click the mailbox that you want to recover and click **Reconnect**.

b In the list of Active Directory accounts, click the user account that you created in step 12 on page 8.12 and click **OK**.

15 Use Microsoft Outlook to export the mailbox data to a .pst file or use the Exmerge.exe tool to extract data from multiple mailboxes.

To download Exmerge.exe, visit the following Microsoft Web site:

http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=429163EC-DCDF-47DC-96DA-1C12D67327D5

8.4.5 Using the Recovery Storage Group Feature

The recovery storage group is a specialized storage group in Exchange. After you restore a mailbox store to the recovery storage group, use the Exmerge.exe tool to move the recovered mailbox data from the recovery storage group to the regular storage group.

8.4.5.1 How Recovery Storage Groups Operate

In previous versions of Exchange Server, a separate Microsoft Active Directory directory service forest needs to be configured on a recovery server if you want to mount another copy of a production Exchange database, or to mount a different version of a production Exchange database. With the Recovery Storage Group feature in Exchange Server, a separate recovery computer is not always needed when you want to recover data from a mailbox store. After you create a Recovery Storage Group, and one or more databases have been added to it, you can either restore online backup sets, or you can copy offline database files to the Recovery Storage Group. To extract or to merge data from recovered databases in the Recovery Storage Group to a mailbox in a regular storage group, use the Exchange Server version of Microsoft Exchange Mailbox Merge Wizard (Exmerge.exe).

To use a Recovery Storage Group, the Active Directory topology of the Exchange Server computer must be intact and must be in the same state as when the copy of the database was made. This means that the mailbox or the mailboxes that you want to recover must not be deleted or purged from the system, or moved to a different database or to a different server.

The Recovery Storage Group feature is not intended for use in disaster recovery operations that involve multiple servers or multiple storage groups. It is intended as a substitute in

situations where previously, an alternative forest recovery server was required. Use the Recovery Storage Group feature in recovery situations where both the following conditions are true:

- The logical information in Active Directory about the storage group and its mailboxes is intact and unchanged.
- You want to recover data from a single mailbox, a single database, or a group of databases that are in a single storage group. For example, you can use a Recovery Storage Group to recover items that were deleted and purged from a user's mailbox, or you can use a Recovery Storage Group to restore or to repair a copy of an alternative database while another copy of the database remains in production.

8.4.5.2 Creating a Recovery Storage Group

To create a Recovery Storage Group:

1. Start the **Exchange Management Console**.
2. Select **Toolbox** on bottom of the left panel.
3. Double-click **Database Recovery Management** in the middle panel.
4. The **Troubleshooting Assistant** window will pop up.
5. Select **Create a recovery storage group**.
6. For the storage group or mailbox database names, select the same name as the storage group and mailbox database names you'd like to recover.
7. Select locations you'd like the recovery storage group files and mailbox database file(s) to reside.
8. Create your recovery storage group.
9. Mount the virtual copy you would like to restore from to the production server.
10. Copy the EDB, CHK, and LOG files to the locations you selected for the recovery storage group.
11. Rename all the CHK and LOG files to have the same header as the Recovery Storage Group. For example if your Recovery Storage Group has a header of R00, then rename all your E00 headers to R00.
12. Mount the Mailbox Database from the **Troubleshooting Assistant**.

13 Select **Merge or copy mailbox contents** and select the specific actions you would like to perform.

8.4.5.3 Restoring a Mailbox Store to the Recovery Storage Group

You can restore a mailbox store to a Recovery Storage Group by manually copying the database files to the appropriate folder on the server.



NOTE: Keep the original backup file in case there is a need to start over.

1 Verify that the database that you want to restore is consistent and that it is in a clean shutdown"state. To do so, open a command prompt, switch to the `ExchSrvr\Bin` folder, type the following line, and then press ENTER:

```
Eseutil /mh YourDatabaseName.edb
```

In the output that appears in the Command Prompt window, note whether the **State** line shows as **State: Clean Shutdown** or **State: Dirty Shutdown**.



NOTE: The following step should have been done after the virtual copy for the storage group was created.

2 Do one of the following, as appropriate to your situation:

a If the database is consistent, go to step 3 on page 8.16.

b If the database is not consistent and if the database log files exist, use the Eseutil.exe tool to perform a soft recovery on the database. When you perform a soft recovery, uncommitted logs are committed to the database. To perform a soft recovery, switch to the ExchSrvr\Bin folder at a command prompt, type the following line, where *rnn* is the log file prefix and *database_folder_path* is the name of the folder where the database files (`.edb`, `.stm`) are located, and then press **ENTER**:

```
eseutil /r rnn /ddatabase_folder_path
```

For example, you might type the following:

```
eseutil /r r00 /d"c:\Program Files\Exchsrvr\Recovery Storage Group"
```



NOTE: There is no space after the `/d` switch.



NOTE: The following step should have been done after the virtual copy for the storage group was created.

3 Immediately after the successful completion of a repair, perform an offline defragmentation of the repaired database. To perform an offline defragmentation, open a command prompt, switch to the `ExchSrvr\Bin` folder, type the following line, and then press ENTER:

```
eseutil /d <YourDatabaseName.edb>
```

4 Copy the `.edb` database files from the virtual copy to the appropriate folders that you specified earlier when you created the Recovery Storage Group.

5 If databases are currently mounted in the Recovery Storage Group, do the following:

a Dismount the databases.

b Use the `Eseutil.exe` tool to verify that the databases are in a clean shutdown state. To do so, open a command prompt, switch to the `ExchSrvr\Bin` folder, type the following line, and then press ENTER:

```
Eseutil /mh YourDatabaseName.edb
```

In the output that appears in the **Command Prompt** window, note whether the **State** line shows as **State: Clean Shutdown** or **State: Dirty Shutdown**. If the databases are consistent, delete all transaction log files (`.log`) and checkpoint files (`.chk`) for the Recovery Storage Group.

6 Start the **Exchange System Manager** and then view the properties of the database that you restored. On the **Database** tab of the **Mailbox Store Properties** dialog box, verify that the **This database can be overwritten by a restore** check box is selected.

7 Mount the database.

To merge data from the recovered databases in the Recovery Storage Group to a mailbox in a regular storage group, use the Exchange Server version of Microsoft Exchange Mailbox Merge Wizard (`Exmerge.exe`).

To download Exmerge.exe, visit the following Microsoft Web site:
http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=429163EC-DCDF-47DC-96DA-1C12D67327D5

8.5 Additional Documentation

See *Recovery Storage Groups* for detailed information that applies to Exchange 2007:

http://technet.microsoft.com/en-us/library/aa997260.aspx

9 Remote Copy for Recovery Manager

In this chapter

9.1 Purpose of Remote Copy **9.1**

9.2 How It Works **9.2**

9.3 Setting Up the Remote Copy **9.3**

9.3.1 Setting Up Remote Copy Groups for Storage Groups **9.3**

9.4 Recovering a Storage Group from a Secondary Site **9.3**

9.5 Synchronous Long Distance Remote Copy Support **9.4**

9.1 Purpose of Remote Copy

3PAR Remote Copy can be used to safeguard against disasters that may occur at one location by keeping a copy of valuable data at another location. For example, if there was a fire or earthquake at a particular location, all of the data stored there could be lost unless a backup copy is maintained somewhere where the data can be recovered. The Remote Copy feature, (supported through the InServ), can prevent this kind of disastrous scenario. When using Remote Copy, two InServs are utilized: a primary that is used for production, and secondary that is used for backup purposes. When disaster strikes in one location, there is always a backup at the secondary site. See the *3PAR Remote Copy User's Guide* for complete information about Remote Copy.

9.2 How It Works

When users want to synchronize the data from the production site to secondary site, Recovery Manager for Microsoft Exchange 2007 freezes the I/O at the application level, and then takes a snapshot of the storage groups and log volumes. Once the snapshot is taken, Remote Copy performs a synchronization on the data changes to the target volumes at the secondary site. After the synchronization is complete, the target server connected to the InServ at the secondary site, creates a virtual copy on the Remote Copy target volumes, and saves the information in its repository at the secondary site.



NOTE: The target server serves as the backup server at the secondary site. After synchronization has completed, a virtual copy will be created and managed by the target server at the secondary site.



NOTE: A virtual copy created on the primary site for Remote Copy purposes will be removed after synchronization has completed.



NOTE: In order for the Recovery Manager GUI to manage virtual copies from the remote target server, you must register the storage group using the exact server name and instance name.



NOTE: In order for successful execution of Remote Copy operations, the InServs in the Remote Copy setup must be configured to be the default InServs using 3PAR's hardware provider tool, `provcfg.exe`. Otherwise, Recovery Manager for Exchange 2007 cannot locate the relevant Remote Copy groups, resulting in the failure of Remote Copy operations.

9.3 Setting Up the Remote Copy

In order to use the 3PAR Remote Copy feature, you must first install and configure a Remote Copy environment.



NOTE: See the *3PAR Remote Copy User's Guide* for details on how to set up Remote Copy.

Once you have Remote Copy set up between two InServs, you should create a Remote Copy group for testing before going to the next step.

9.3.1 Setting Up Remote Copy Groups for Storage Groups

Follow these steps to set up Remote Copy for a given storage group:

1. Identify the volumes that contain the storage group and log files to be copied.
2. Create one Remote Copy group for one mailbox database.
3. Add the volumes belonging to the storage group files and log files into the Remote Copy group with Remote Copy target volumes.
4. Synchronize the Remote Copy group.

Every storage group's log and database file should be added in one Remote Copy group. Two or more storage groups in one Remote Copy group are not supported. DB files from the same storage group and log files from the same stroage group located in the different Remote Copy group are not supported.

If the storage group is not in the Remote Copy group the Remote Copy feature cannot be used.

9.4 Recovering a Storage Group from a Secondary Site

In the event of a storage group crash at a primary site, you should have a dedicated target server at the secondary site that is setup in an identical manner to the original production server for recovery purposes (same configuration includes instance names, database names, structures, and with Windows authentication mode set in the same way as well).

You can use the backup server of Recovery Manager for Microsoft Exchange 2007 at the secondary site with the following procedure:

1. Mount the virtual copy to the production server.
2. Log onto the production server, stop the Exchange instance and its dependent services.
3. From the mounted snapshot volumes, manually copy all necessary storage group and log files to the corresponding storage group location.
4. Re-start the Exchange instance and its dependent services.
5. Log back onto the backup server, unmount the virtual copy.

9.5 Synchronous Long Distance Remote Copy Support

Synchronous Long Distance Remote Copy in synchronous mode and periodic mode is supported. The Recovery Manager target server should have connectivity to the InServ in periodic mode.



NOTE: If you are performing a promote restore for volumes in a Synchronous Long Distance Remote Copy relationship, you must manually stop Remote Copy before initiating the volume promote restore.

A
Server Virtualization Environments

A.1 VMWare and Egenera

Support for VMWare and Egenera environments is provided under certain specific conditions. New volumes presented to VMWare and Egenera servers are not surfaced automatically, so the `RMExch mount` command is limited to being executed on the backup host. Figure A-1 on page A.2 shows the relationships between the InServ and VMWare and Egenera in a virtualization environment:

3PAR Confidential

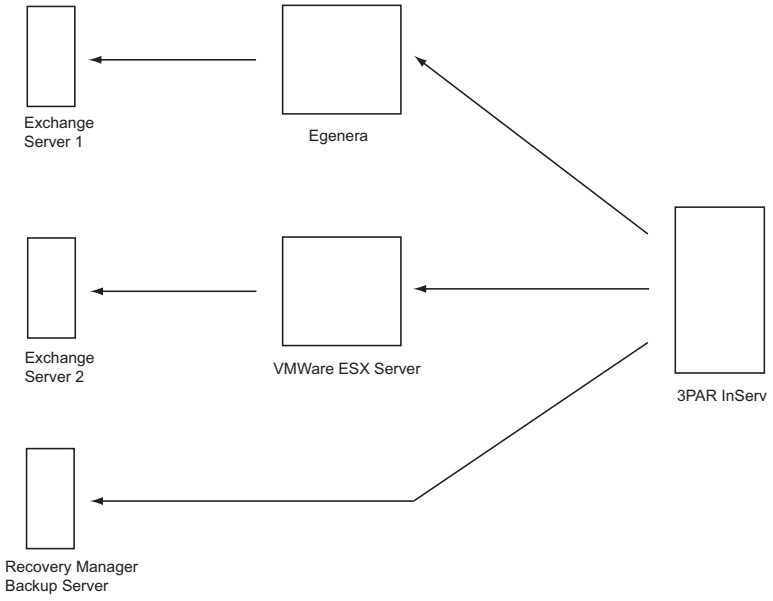


Figure A-1. Sever Virtualization Environment

The following requirements need to be met for VMWare and Egenera to be supported:

1. The disks presented to the Exchange Servers need to be raw devices.
2. The backup server needs to be connected directly to the InServ and not through VMWare or Egenera.

- The `RMExch mount` command can not be run against a virtual machine from the VMWare or Egenera server with the `-h` option.



NOTE: The `-expose` option has been deprecated and will be removed in a future release.

- The `RMExch mount` command with the `-expose` option, can be used in this case.
- If `RMExch mount` with the `-expose` option is not used, the storage administrator needs to perform the actions to expose the volumes to the server manually.

Due to these restrictions, restores performed in these virtualized environments require a different set of steps than shown in Chapter 8, *Rapid Backup and Recovery for Exchange*. Filecopy and volume promote restores are not supported for virtualized environments.

Here are the steps to perform a restore:

1. Follow steps 1 through 4 in *Point-In-Time Recovery* on page 8.4.
2. Mount the virtual copy to the backup server or restore it from backup media to the production server.
3. On the production server, move the .edb, .log, and .chk files from the original locations to another location. The original locations can be determined from the Exchange Management Console.
4. Copy the .edb, .log, and .chk file(s) from the mounted or restored virtual copy location to the actual database location.

B Troubleshooting

B.1 Known Issues

- If a VV name on the InServ is changed, the virtual copy taken before the name change will not be able to perform a volume promote restore.
- For media backup virtual copy, it is recommended that a policy be maintained per storage group to avoid the possibility of having the batch file overwritten under some conditions.
- When upgrading an update rollup patch on Exchange 2007 and executing a snapshot creation with the validate (-VS) option without re-logging the console, an application error message is displayed. To avoid this error, log off and log in after the update.

B.2 Known Microsoft Issues

- On a computer that is running a clean installation of Windows Vista Service Pack 1 (SP1) or Windows Server 2008, an event ID 10 may be logged in the System log by VDS Dynamic Provider. Please refer to the following website for more details:

  http://support.microsoft.com/kb/948275

- Under some conditions, there may be a problem when deleting folders on directory mounted Virtual Volumes. This is a Windows know issue. Please refer to the following web site:

  http://support.microsoft.com/?kbid=319368

B.3 Troubleshooting

This appendix is designed to be used like a Frequently Asked Questions section. It will help find solutions to some of the common issues that may arise when running Recovery Manager for Exchange.

NOTE: Recovery Manager for Exchange depends on the VSS Framework and the Microsoft Exchange writer to be in a good state to function properly. If a problem occurs, check the status of the Exchange Writer with the command `vssadmin list writers`. The state of the Microsoft Exchange writer should be 'stable' (for the Replication Writer in CCR configurations). If it is not stable, find a good time to restart the Information Store service. You may also need to restart the VSS Service.

Problem:

You may get the following message when operating in the Windows 2008 environment while executing **Create VC** or **Mount VC** with the **Disk Management** window open.



Suggestion:

This popup can be ignored by clicking **Cancel** as advised by Microsoft on their support site:

http://support.microsoft.com/kb/969601.

Problem:

The virtual copy creation always fails on storage group integrity checking.

Suggestion:

Make sure that the Exchange management tool on all Recovery Manager for Exchange installed hosts have the same service pack installed.

Problem:

Recovery Manager is running on both backup and server production server but Recovery Manager consistently fails to issue a command to the remote system.

Suggestion:

Make sure the communication port for Recovery Manager is set to be the same on all Recovery Manager installed systems. You need to restart the Recovery Manager for Exchange Agent service on every system followed by the `port change` command. If the firewall or security monitoring software is installed, verify that the communication port and remote registry service ports (139 and 445) are allowed for access.

Problem:

Recovery Manager cannot locate the Exchange Server.

Suggestion:

Recovery Manager uses the Active Directory structure to locate Exchange server information within the same domain. Recovery Manager will not be able to access the Exchange information if it is not in the same domain.

Problem:

Recovery Manager cannot detect the storage group.

Suggestion:

The Recovery Manager user has to have Exchange Administrator privilege to access Exchange active directory objects.

Problem:

Virtual copy creation always fails on the storage group.

Suggestion:

There are a few things to check on your system.

1. Make sure both the data and log files of your storage group are installed on 3PAR volume.
2. Make sure your 3PAR volume is formatted as Basic Disk type.

3 Make sure you have allocated snapshot space for your 3PAR volumes.

4 Make sure your system configuration conforms to the 3PAR support matrix.

Problem:

The Recovery Manager interface takes a long time to start or to bring up the server registration dialog.

Suggestion:

When Recovery Manager is started for the first time, or when you click on the server registration, Recovery Manager will try to scan the entire network for available Exchange servers. Exchange object query might cause this latency.

Problem:

Recovery Manager always fails to issue a command from the user interface and command line right after the installation.

Suggestion:

If the software is installed through a remote desktop session, the newly added environment variables will not become effective until you log off the session. If the software is installed directly from the system console, these variables should be available immediately.

Problem:

NetBackup takes a substantial amount of time to start a backup process. However, Recovery Manager claims that the backup has failed.

Suggestion:

Timeout for backup initialization detection can be modified to accommodate the timing issue. Please refer to the `RMExch config` command for more information.

Problem:

NetBackup takes a substantial amount of time to complete a backup process.

Suggestion:

Make sure you have the latest maintenance package installed for your NetBackup application. Please refer to the latest Configuration Matrix for the appropriate information.

Problem:

`RMExch` cannot connect to the specified server.

Suggestion:

Make sure the Recovery Manager for Exchange Agent service is started and that the port settings on all Recovery Manager installed systems are the same. If you changed the port setting, you need to restart the Recovery Manager for Exchange Agent service before running any command.

Problem:

`RMExch create` is not creating a virtual copy.

Suggestion:

Check to see if you have reached the number of virtual copies allowed by your policy for this Exchange server. Also check if the oldest virtual copy is mounted, as this will not allow a create if the maximum number of virtual copies has been reached.

Problem:

The mounted virtual copies always show up as read-only.

Suggestion:

Make sure the Virtual Disk Service is not disabled on your system. If this service is disabled, Recovery Manager will not be able to make the virtual copy writable.

Problem:

Recovery Manager fails to create a virtual copy for a storage group on the 3PAR volume which is also a system drive.

Suggestion:

Performing a snapshot of a storage group on the system volume is currently not supported by Recovery Manager for Exchange.

Problem:

Recovery Manger shows the "Error - VSS Asynchronous operation failed. It is recommended that you wait 10 minutes and then try the operation again" message when the `create` command is executed.

Suggestion:

When you encounter this error message, run the `vssadmin list writers` command to list all of the available writers on the system that are taking the snapshot of the Exchange storage

group. Make sure the Microsoft Exchange Writer status is stable. If the status is other than stable, you need to restart the Exchange server service to reset the writer status.

Problem:

Recovery Manager shows the `ERROR: Failed - Virtual Copy creation failed for storage group <StorageGroup>` message after an unexpected termination of the virtual copy create process.

Suggestion:

When Recovery Manager unexpectedly terminates, an internal locking file might still exist on your Exchange server system. You need to remove the locking file manually for the create process to run through. The locking file can be located under: `<InstallationPath>\Exchange\vclock`. Use the `rmexch reset` command to reset the lock.

Problem:

The event viewer shows the `Volume Shadow Copy Service error: Unexpected error IOCTL_STORAGE_QUERY_PROPERTY(\\.\PHYSICALDRIVE2, StorageDeviceProperty) - BuildLunInfoForDrive. hr = 0x80070002.` error when a virtual copy creation is in progress.

Suggestion:

When this message is logged by the Volume Shadow Copy service, it notifies the user that the initial search on the imported volume is not complete. It will try again to make sure the snapshot can be imported successfully. If the snapshot process still fails and this error is logged, please contact 3PAR.

Problem:

Recovery Manager creates the virtual copy successfully but does not show it in GUI or in CLI.

Suggestion:

If the virtual copy is requested on a passive from active node or vice versa, it will be created on the desired node. The virtual copy is visible only on the node where it is created. Check the appropriate node.

Problem:

Recovery Manager shows a virtual copy as available but it is mounted or vice versa.

OR

Recovery Manager shows a virtual copy as available but still it still cannot be mounted as the status indicates that the virtual copy is already mounted.

Suggestion:

This mismatched entry might be due to a previously failed Recovery Manager operation(s). Check the mismatched entries using the `analyze` command.

To resolve these entries, follow the steps detailed below:

1. Remove VLUNs and VVs for the mismatched volume.

Run: `RMExch analyze -s <exchange server> -g <storage group>`

This command will show which VVs and VLUNs may be left over from a previously failed operation. Remove these VLUNs and VVs manually from the InServ.

2. Remove timestamp entries from the repository.

Run: `RMExch analyze -s <exchange server> -g <storage group>`

This will show all `Missing VVs` from a storage group. These are the VV entries that are deleted from InServ but are still in the repository. Remove the respective timestamps from repository by deleting the directory:
`<installpath>\3PAR\RM\Exchange\Repository\<exchange server>\<storage group>\<time stamp>`

Problem:

Recovery Manager takes too long to create a virtual copy .

Suggestion:

Once the snapshot is created, it is verified and .log files are truncated. For this, checkpoint is fetched and log file names are traversed one by one. This may take a longer due to a large number of `.log` files for a storage group. If a virtual copy creation is taking too long, check the virtual copy creation with the -nc switch. This will skip log verification and log truncation. Then, verify this snapshot using the `validate` command. Once it is validated, to truncate logs, create a snapshot using the `-truncate` and `-nc` switches. Now, try a regular virtual

copy creation. If the virtual copy creation with `-nc` is also taking a longer time, please send an RMReport to 3PAR Customer Support.

Problem:

After installing RME 4.1.0, it is unable to manage Exchange cluster from Exchange management. It returns a COM class factory error.

OR

After installing RME 4.1.0, an MSCluster related COM class factory error is returned.

Suggestion:

If RME 3.0.0.* is uninstalled, the msclus.dll is unregistered and results in the COM class factory error. To resolve this, run:

```
- regsvr32 C:\Windows\system32\msclus.dll
```

Problem:

How to recover the Exchange writer status from last error `Non-retryable` to `No error`.

Suggestion:

If the Exchange writer status shows the last error as `Non-retryable` on a CCR active or passive node or an LCR passive copy, try one of the following methods to get the writer into a stable state with no last error.

Restart Microsoft Exchange Replication service from passive node.

OR

```
Net stop MSExchangeRepl
Net start MSExchangeRepl
```

If restarting the Microsoft Exchange Replication service does not solve the problem, try one of the following methods:

Restart Microsoft Exchange Information Store service.

OR

```
Net stop MSExchangeIS
Net start MSExchangeIS
```

Problem:

How to recover the System Writer status from last error `Non-retryable` to `No error`.

Suggestion:

Restart the Cryptographic Services service.

OR

```
Net stop CryptSvc
Net start CryptSvc
```

Problem:

Remote Copy status for the group <remote copy group> does not permit synchronization.

Suggestion:

The involved Remote Copy group has virtual volumes that are not in synced state. Wait until all volumes in the group appear in synced state and then retry the operation.

Problem:

An LDP COM error message appears similar to the following:

RME5220: ERROR: COM: Failed to bind to LDAP path <CN=Recovery Storage Group,CN=InformationStore,CN=WWDC1-EX-CPBE01,CN=Servers,CN=Denver,CN=Administrative Groups,CN=Westwood,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=westwood2000>: 0xc1032221.

Suggestion:

You may not have permissions for the specified storage group, or the storage group is absent.

C
Event Messages

C.1 Description of Events

This appendix provides information for all of the events generated by 3PAR Recovery Manager 4.1.0 for Microsoft Exchange 2007.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages

Event ID	Error Message	Description/Action
3006	RME3006: ERROR: 3PAR VSS provider not found, exiting.	3PAR VSS Provider could not be located. ■ Verify the 3PAR VSS Provider installation from Add/Remove programs. ■ If VSS Provider is installed, run `vssadmin list providers` to check that 3PAR VSS Provider is installed properly.
3056	RME3056: ERROR: One of the drives is not a 3PAR volume.	Some of the target volumes are not 3PAR virtual volumes. All of the drives need to be 3PAR drives. ■ Verify that all database and log destinations belong to a 3PAR storage system.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
3076	RME3076: ERROR: You have reached the maximum number of virtual copies allowed for the current policy. Please delete one or update the policy to allow deletion of oldest virtual copies.	The maximum number of virtual copies for the current policy has been reached. ■ Delete the existing virtual copy. ■ Modify the policy to allow more virtual copies for a storage group or to delete older copies.
3077	RME3077: ERROR: The maximum number of virtual copies <Max. Count> has been reached for Exchange Server <Server Name> policy and the oldest Virtual Copy is currently mounted. Please unmount this Virtual Copy before creating another Virtual Copy.	The maximum number of virtual copies for the specified Exchange Server policy has been reached. ■ Unmount the oldest virtual copy to have it deleted during virtual copy creation. ■ Modify the policy to allow more virtual copies for a storage group.
3112	RME3112: ERROR: Your database is spread across multiple InServs on the production server. Please move the storage group to only one InServ and perform this operation again.	The storage group is spread across multiple InServs. ■ The database or log target volume must belong to a single InServ. Refer to the preferred configuration setup.
3122	RME3122: ERROR: Unable to configure peer backup server.	Failed to save the information to the configuration file. ■ Check that you have right permissions to the RMExchange Repository directory.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
3126	RME3126: ERROR: Could not delete the local configuration file.	Failed to save the information to the configuration file. ■ Check that you have right permissions to the RMExchange Repository directory.
3137	RME3137: ERROR: The Exchange server is set to include all storage groups. Please remove this umbrella to register individual Storage Groups.	The Exchange server cannot determine which specific storage groups to set up as the current range is to wide. ■ Unregister all storage groups and then register only the desired groups one by one.
3150	RME3150: ERROR: The zip file already exists.	The specified zip file already exists. ■ Change the zip file name or delete the existing zip file.
3151	RME3151: ERROR: The filename must end with .zip.	An invalid filename format was specified for the zip file. ■ Check the syntax for the zip filename specified through the `RMExch report` command.
3155	RME3155: ERROR: Missing storage group name.	The storage group name is missing from the `RMExch` command syntax. ■ The storage group name must be included in the `RMExch` command parameters.
3157	RME3157: ERROR: Number of virtual copies need to be in the range of 1 to <Max. Count>.	The number of virtual copies is out of the range specified by the current policy. ■ Reduce the number of virtual copies for this procedure or modify the policy for the appropriate number of virtual copies by raising the maximum count level.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
3158	RME3158: ERROR: Invalid parameter entered for policy command.	An invalid parameter was specified for the `RMExch policy` command. Check the syntax for the `RMExch policy` command for the correct parameters.
3164	RME3164: ERROR: There is a conflict with the specified path for repository relocation.	A conflict was detected with the specified repository relocation path. ■ Verify the paths given for repository relocation.
3168	RME3168: ERROR: The replication status of a storage group is '<Status>'. A copy of unhealthy storage group cannot be made.	A copy process was not completed due to the status of the storage group. ■ Check the storage group status. Get it into a Healthy state and then try to create a copy.
3169	RME3169: ERROR: One of the databases in the storage group may be dismounted, cannot continue with Virtual Copy creation.	A Virtual Copy creation could not be completed due to a possible database dismount in the associated storage group. ■ Mount all the databases in a storage group and try to create the virtual copy.
3173	RME3173: ERROR: The Virtual Copy is not found in the repository, check if parameters are correct.	The specified virtual copy could not be located in the repository. ■ Check the syntax for the `RMExch backup` command.
3176	RME3176: ERROR: Verification has encountered an error. Please run Validate command on this snapshot.	A verification error for the snapshot operation has occurred. ■ Run `RMExch validate` to verify that the snapshot was created.
3198	RME3198: ERROR: Backup error occurred. Check to see if your policy name is correct.	An error has occurred during the backup. ■ Check the `RMExch backup` command parameters to ensure that the correct policy name is used.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
3200	RME3200: ERROR: NetBackup process has failed with error code <Error Code>. Check if NetBackup is included in environment variable "PATH". Consult NetBackup manual for this error code.	The NetBackup process has generated an error. ■ Verify that NetBackup is installed properly and verify that the bin sub-folder is specified in the PATH environment variable. ■ Refer to the NetBackup documentation for information on the returned error code.
3204	RME3204: ERROR: Two or more files of this storage group share volume(s). Please unmount the shared volume(s) before proceeding.	Multiple files from the storage group share volumes. ■ Check the file path and volume mapping to determine which volume is shared with the other storage group(s). Unmount this shared volume.
3205	RME3205: ERROR: Mount this Virtual Copy before running restore.	The Virtual Copy was not mounted before running restore. ■ Mount the virtual copy and then try file-copy restore.
3206	RME3206: ERROR: Unmount this Virtual Copy before running promotion restore.	The Virtual Copy was not unmounted before promoting the restore. ■ Unmount the virtual copy and then try promoting the restore.
3210	RME3210: ERROR: Unmount all mailbox stores within a storage group before attempting a restore.	All mailbox stores within the storage group were not unmounted before attempting a restore. ■ Unmount all mailboxes in the storage group and then try to restore.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
3212	RME3212: ERROR: Unmount all public folder stores within a storage group before attempting a restore.	All public folder stores within the storage group were not unmounted before attempting a restore. ■ Unmount all public folder stores in the storage group and then try to restore.
3213	RME3213: ERROR: All databases in the storage group must be dismounted to perform a restore.	All databases in the storage group were not unmounted before attempting a restore. ■ Unmount all databases in the storage group and then try to restore.
3216	RME3216: ERROR: Promotion of volume <Volume Name> failed.	Promotion of the specified volume has failed. ■ Consult the windows event log for the specific error message.
3220	RME3220: ERROR: The backup you would like to restore is not found. Please check your parameters.	A restore for the specified backup could not be performed. ■ Check the syntax for the `RMExch backup` command.
3501	RMCOMN3501: ERROR: The volume is spread across multiple InServs. This configuration isn't supported.	The database or log target volume cannot be spread across multiple InServs as this configuration is not supported. ■ Refer to the preferred configuration setup.
3801	3PARVSS3801: ERROR: Invalid timeout value specified. The valid range is <number 1> to <number 2> seconds.	An invalid timeout value has been specified. ■ Verify that specified timeout value is within the supported range of 3 minutes (180 sec) to 10 minutes (600 sec).
3802	3PARVSS3802: ERROR: Invalid retry value specified. The valid range is <number 1> to <number 2>.	An invalid retry value has been specified. ■ Verify that specified retry value is within the supported range of 0 to 10.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
3803	3PARVSS3803: ERROR: Unable to access connection setup.	The connection setup could not be accessed. ■ Verify that the 3PAR VSS Provider Registry Key is still valid on the system. If the Registry Key cannot be found, reinstallation is required.
3804	3PARVSS3804: ERROR: Unable to find configuration for InServ Storage System <Inserv Name>.	The configuration information for the specified InServ could not be located. ■ Verify that the correct InServ name is entered for the inquiry.
3805	3PARVSS3805: ERROR: Can not remove default InServ Storage System configuration. You need to select another InServ Storage System configuration as default entry before removing this configuration.	Removal of the currently designated default InServ configuration is not allowed. ■ Designate another InServ Storage System configuration as the default before performing this operation.
3806	3PARVSS3806: ERROR: Unable to read InServ Storage System node name entry from registry.	The specific InServ configuration information can not be located in the registry. ■ Try re-registering the InServ Storage System Configuration again using the appropriate 3PAR VSS Provider cli command. Consult the VSS Provider documentation for details.
3807	3PARVSS3807: ERROR: Unable to read InServ Storage System password file path entry from registry.	The specific InServ password file information can not be located. ■ Try re-registering the InServ Storage System Configuration again using the appropriate 3PAR VSS Provider cli command. Consult the VSS Provider documentation for details.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
3808	3PARVSS3808: ERROR: Unable to access InServ Storage System connection setup.	The specific InServ connection information cannot be located. ■ Make sure you have proper permission to access the registry. ■ Try re-registering the InServ Storage System Configuration again using the appropriate 3PAR VSS Provider cli command. Consult the VSS Provider documentation for details.
3809	3PARVSS3809: ERROR: Invalid input for '-sockssl' option.	An invalid input has been specified for the `-sockssl` option. Verify that the specified input is supported.
3810	3PARVSS3810: ERROR: Process has failed to create the password information. Please make sure you have entered the correct information.	Unable to access the specified InServ. ■ Make sure you have entered the correct InServ name and user authentication information.
3811	3PARVSS3811: ERROR: Unable to access generated password information.	Unable to generate password information for the configuration. ■ Make sure you have a proper connection to the InServ.
3812	3PARVSS3812: ERROR: Unable to verify credential information.	The authentication information could not be verified. ■ Check that the specified authentication information is valid and up-to-date. ■ If the original user account or password on the InServ has been modified, you need to run the configuration tool again to update the cached information.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
3813	3PARVSS3813: ERROR: Unable to get InServ Storage System information. Please make sure you have entered the right information and have proper access right.	The InServ information could not be retrieved. ■ Make sure you have entered the right information and have proper access rights. ■ Check if there is any issue with your network connection to the InServ storage system.
3814	3PARVSS3814: ERROR: Unable to find license information in the target InServ Storage System. Please make sure you have entered the right information.	The InServ license information could not be located for the target InServ. ■ Make sure you have entered the correct information and have proper access rights. ■ Check if there is any issue with your network connection to the InServ storage system.
3815	3PARVSS3815: ERROR: Unable to find VSS Provider license in the target InServ Storage System. Please make sure you have entered the right information.	The VSS Provider for Microsoft Windows license information could not be located. ■ The "VSS Provider for Microsoft Windows" license is required on the target InServ Storage System. ■ Contact 3PAR Sales/Support for licensing assistance.
3816	3PARVSS3816: ERROR: Unable to find Virtual Copy license in the InServ Storage System. Please make sure you have entered the right information.	The Virtual Copy license information could not be located for the InServ. ■ The "Virtual Copy" license is required on the InServ Storage System. ■ Contact 3PAR Sales/Support for licensing assistance.
3817	3PARVSS3817: ERROR: VSS Provider license has already expired. Please contact 3PAR support for assistance.	The "VSS Provider for Microsoft Windows" license has expired on the target InServ Storage System. ■ Contact 3PAR Sales/Support for licensing assistance.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
3818	3PARVSS3818: ERROR: Unable to encrypt/decrypt authentication data. Additional information: <Exception Message>.	The authentication data has been corrupted on your system. ■ Re-run the configuration setup for this specific InServ.
3819	3PARVSS3819: ERROR: Invalid log level specified. The valid range is 1 to 5.	An invalid log level has been specified. ■ Make sure the specified log level range is from 1 to 5.
3820	3PARVSS3820: ERROR: Unable to access log level setup.	The log level setup could not be accessed. ■ Make sure you have the proper permission and privilege to access the registry setup.
3821	3PARVSS3821: ERROR: Fail to spawn an InForm CLI process.	An attempt to spawn an InForm CLI process has failed. ■ Make sure you have InFormCLI installed on your system and that it is registered in the system environment variable's PATH.
3822	3PARVSS3822: There is no existing InServ Storage System configuration entry.	No existing InServ configuration entry could be located. ■ You must have at least one InServ configuration entry. ■ Use the configuration tool to add the appropriate entry to the list.
5050	3PARVSS5050: ERROR: Unsupported feature <Feature Name>.	The specified volume snapshot attribute is not supported by 3PAR VSS Provider. ■ Please refer to the latest version of the 3PAR VSS Provider for Microsoft Windows User's Guide for a list of supported features.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5051	3PARVSS5051: ERROR: The shadow copy set has exceeded the maximum number (64) of allowable volumes.	Microsoft VSS only allows a maximum of 64 volumes to be participated in a snapshot process.
5052	RM5052: ERROR: Could not allocate memory.	This type of memory allocation failure can result from a system wide contention for resources. ■ Check the event log for more detailed information.
5053	3PARVSS5053: ERROR: Could not communicate with the 3PAR InForm CLI.	This problem can be caused by an incorrect authentication setup, unavailability of an InFormCLI tool, or a licensing issue. ■ Verify the 3PAR InFormCLI installation. ■ Check to make sure the bin sub-folder is in PATH. ■ Check the Application Log of the Event Viewer for more information.
5054	3PARVSS5054: ERROR: CLI: <command>.	The command submitted to InFormCLI has generated an error. ■ Check the Application Log of the Event Viewer for more information.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5055	3PARVSS5055: ERROR: <Token>: Invalid token.	Unable to identify requested information received from the InServ. ■ Check that your InServ version is supported by 3PAR VSS Provider and that there are no network problems that could result in a partial data transmission. ■ To determine the version for a particular InServ, run the `showversion` command. ■ For the 3PAR VSS Provider version, run `"vssadmin list providers"` and check the 3PAR VSS Provider entry that specifies the version and other details.
5056	3PARVSS5056: ERROR: Could not open volume mapping file: <Volume Map File>.	Unable to build the internal virtual volume database. ■ Check that your InServ version is supported by 3PAR VSS Provider and that there are no network problems that could result in a partial data. transmission. ■ To get the version for a particular InServ, run `showversion`. ■ For the 3PAR VSS Provider version, run `"vssadmin list providers"` and check the 3PAR VSS Provider entry that specifies the version and other details.
5057	3PARVSS5057: ERROR: Could not open file: <File Name>.	Unable to open the designated file for internal processing. ■ Check that you have the proper privilege to access the Windows temporary folder.
5058	3PARVSS5058: ERROR: Could not create file: <File Name>.	Unable to create the designated output file for internal processing. ■ Check that you have the proper privilege to access the Windows temporary folder.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5059	3PARVSS5059: ERROR: SYSTEM: <Error Code &/or Description>.	A windows system decode error code has been generated. ■ To get a more detailed description, consult msdn.microsoft.com or Windows help.
5061	3PARVSS5061: ERROR: IOCTL inquiry call failed.	Unable to perform an inquiry on the targeted volume. This might be caused by specifying an invalid volume during snapshot creation. ■ Make sure all volumes participated in the snapshot process are valid and 3PAR storage volumes. ■ Check to see that the volumes are accessible and are not in a bad or offline state.
5062	RM5062: ERROR: Could not query windows registry key <Registry Key>.	Unable to access registry for the specified key name. ■ Use `regedit` to check that the registry still has the corresponding key and that you have the proper permission to access it.
5063	3PARVSS5063: ERROR: Could not query windows registry key name <Registry Key>.	Unable to access the registry for the specified key name. ■ Use `regedit` to check that the registry still has the corresponding key and that you have the proper permission to access it.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5064	RM5064: ERROR: Could not open windows registry key for 3PAR VSS Provider.	Unable to access the registry for the 3PAR VSS Provider installation. ■ Verify the 3PAR VSS Provider installation from Add/Remove program or run `vssadmin list providers`. ■ Check that the registry still has the corresponding key and that you have proper permission to access it. If this key is missing, you need to reinstall the 3PAR VSS Provider package.
5065	3PARVSS5065: ERROR: Target LUN <Lun Id> is not a 3PAR Virtual Volume.	The designated target LUN is not a 3PAR virtual volume. ■ Verify that all database and log destinations belong to the 3PAR storage system.
5066	3PARVSS5066: ERROR: Target LUN <Lun Id> could not be identified.	The specified target volume does not have adequate device information for proper identification.
5067	3PARVSS5067: ERROR: Destination LUN <Lun Id> could not be identified.	The specified destination volume does not have adequate device information for proper identification.
5071	3PARVSS5071: ERROR: Unexpected snapshot set ID at <Server Name>.	An unexpected snapshot set ID was encountered during the snapshot set preparation. ■ Restart both Volume Shadow Copy Service and 3PAR VSS Provider Service to reset the status.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5072	3PARVSS5072: ERROR: <Error Code> call out of order.	The internal VSS call stack is not in the correct order. ■ Restart both Volume Shadow Copy Service and 3PAR VSS Provider Service to reset the status.
5073	3PARVSS5073: ERROR: Could not detect 3PAR InForm CLI installation.	Unable to get the InFormCLI registration information for the local system. ■ Verify the InFormCLI package installation from Add/Remove Programs. ■ Verify registry keys for the InForm CLI installation.
5102	RME5102: ERROR: The VSS Writer ran out of memory or other system resources. The recommended way to handle this error is to wait ten minutes and then repeat the operation. If the VSS Writer is in a bad state, restart the writer's service. Check the application event log.	A resource allocation error has occurred during a VSS Writer operation. ■ Try waiting 10 minutes and then retry the operation. ■ Run `vssadmin list writers` to verify that the VSS writer is in Healthy state.
5103	RME5103: ERROR: The VSS Writer operation failed because of a time-out between the Freeze and Thaw events.	The VSS Writer operation has exceeded the 20 second time-out limit for the freeze and thaw stage allocated by Exchange. ■ Verify that the Exchange writer is in a healthy state using `vssadmin list writers`.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5104	RME5104: ERROR: The VSS Exchange Writer has failed. This can be verified by running the command "vssadmin list writers" from the command line. To put it into a stable state and to continue creating snapshots, restart the Microsoft Exchange information store.	The VSS Exchange Writer has failed. ■ This can be verified by running the `vssadmin list writers` command from the command line. ■ You may need to restart the VSS service and/or Exchange Information Store service.
5106	RME5106: ERROR: The VSS Writer is not responding.	The VSS Writer is not responding. ■ Run `vssadmin list writers` to verify that the VSS writer is in a healthy state.
5108	RME5108: ERROR: The VSS Writer infrastructure is not operating properly. Check that the Event Service and VSS have been started, and check for errors associated with those services in the error log.	The VSS Writer is not operating properly. ■ Check that the Event Service and VSS have been started. ■ Run `vssadmin list writers` to verify that the VSS writer is in a healthy state and check the system event log for errors associated with those services.
5111	RME5111: ERROR: The 3PAR VSS Provider is not registered on this computer.	A registered version of VSS Provider was not detected. ■ Check that 3PAR VSS Provider is properly installed on the system. ■ Run `vssadmin list providers` to verify that 3PAR VSS provider is properly registered. ■ If you cannot resolve the problem, uninstall the 3PAR VSS Provider package and install it again.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5112	RME5112: ERROR: An unexpected 3PAR VSS Provider error occurred.	An unexpected error was generated by VSS Provider. ■ Restart the Volume Shadow Copy Service and 3PAR VSS Provider service.
5113	RME5113: ERROR: The VSS Provider is in use.	Another snapshot request is currently in process. ■ Wait 10 minute and re-try the operation.
5118	RME5118: ERROR: An unexpected VSS provider error has occurred.	An unexpected error was generated by VSS Provider. ■ Check the Windows event log to determine the specific VSS Provider error.
5121	RME5121: ERROR: Could not bind to the domain for Exchange Server Information.	A domain binding error has occurred while accessing the Exchange Server Information. ■ Check the Active Directory connection.
5122	RME5122: ERROR: The system was unable to flush I/O writes. This can be a transient problem. It is recommended to wait ten minutes and try again, up to three times.	The system was unable to flush I/O writes. This can be a transient problem. ■ Try waiting 10 minutes and try again, up to three times. ■ If the operation cannot be instigated after three retries, run `vssadmin list writers` to verify that the VSS writer is in a healthy state.
5123	RME5123: ERROR: The system was unable to hold I/O writes. Try again when the Exchange Server is not as busy.	The system was not able to process I/O writes. ■ Try again when the Exchange Server is not as busy. ■ Run `vssadmin list writers` to verify that VSS writer is in a healthy state.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5126	RME5126: ERROR: The creation of a shadow copy is in progress, and only one shadow copy creation operation can be in progress at one time.	The system was unable to complete the shadow copy operation as another snapshot request was being processed. Additional information can be found in the Application event log. ■ Wait 10 minute and re-try the operation.
5127	RME5127: ERROR: A NetBackup operation is already in progress, and only one NetBackup operation at a time is allowed.	Another NetBackup request is in process, and only one backup operation at a time is allowed. ■ Re-try the operation.
5128	RME5128: ERROR: Cannot find the Virtual Copy in the Repository.	The Repository might be out of sync. ■ Run `RMExch analyze` to determine the out-of-sync entries. ■ (See Chapter B, *Troubleshooting* for more details.
5134	RME5134: ERROR: removevlun operation failed.	The `removevlun` operation has failed. ■ Check to see if you can connect to the required InServ from the CLI command window.
5135	RME5135: ERROR: createvlun operation failed.	The `createvlun` operation has failed. ■ Check to see if you can connect to the required InServ from the CLI command window.
5136	RME5136: ERROR: removevv operation failed.	The `removevv` operation has failed. ■ Check to see if you can connect to the required InServ from the CLI command window.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5137	RME5137: ERROR: showvv operation failed.	The `showvv` operation has failed. ■ Check to see if you can connect to the required InServ from the CLI command window.
5138	RME5138: ERROR: createsv operation failed.	The `createsv` operation has failed. ■ Check to see if you can connect to the required InServ from the CLI command window.
5139	RME5139: ERROR: promotesv operation failed.	The `promotesv` operation has failed. ■ Check to see if you can connect to the required InServ from the CLI command window.
5142	RME5142: ERROR: showhost operation failed.	The `showhost` operation has failed. ■ Check to see if you can connect to the required InServ from the CLI command window.
5143	RME5143: ERROR: showvlun operation failed.	The `showvlun` operation has failed. ■ Check to see if you can connect to the required InServ from the CLI command window.
5144	RME5144: ERROR: 3PAR <Recovery Manager component> license has expired. Contact 3PAR representatives to acquire a new license.	The licence for a Recovery Manager component appears to have expired. ■ Check to see if there is a communications problem by connecting to the required InServ from the CLI command window. ■ Check the validity of the Recovery Manager License for the InServ using the `showlicense` command.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5145	RME5145: ERROR: Could not retrieve 3PAR <Recovery Manager component> license. Contact 3PAR representatives to acquire a valid license.	The licence for Recovery Manager component could not be verified. ■ Check to see if there is a communications problem by connecting to the required InServ from the CLI command window. ■ Check the validity of the Recovery Manager License for the InServ using the `showlicense` command.
5146	RME5146: ERROR: Datastore '<Datastore Name>' is already mounted to host '<Host Name>'.	The selected Virtual Copy has already been mounted to the specified host.
5147	RME5147: ERROR: Cannot remove a mounted virtual copy. Please unmount it and try again.	A mounted virtual copy could not be removed. ■ Unmount the virtual Copy before deleting it.
5151	RME5151: ERROR: The VSS Provider does not appear to be installed. You cannot create a Virtual Copy without the provider. Please Check the VSS provider installation.	VSS Provider does not appear to be installed. ■ Verify the proper 3PAR VSS Provider installation via the Add/Remove program or run the `vssadmin list providers` command to verify the installation.
5152	RME5152: ERROR: Creating this Virtual Copy will exceed the maximum number of Virtual Copies allowed by the Policy. Maximum number of Virtual Copies is set to '<Max. VC count in Policy>'.	The maximum number of Virtual Copies has been exceeded. ■ Check the policy setting for the particular storage group. If the option for retaining the oldest virtual copy is set, subsequent Virtual Copy creation will not be allowed after it reaches the maximum limit.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5155	RME5155: ERROR: NetBackup restore process has failed.	The NetBackup restore has failed. ■ Check application event log and netbackup logs on the netbackup server.
5156	RME5156: ERROR: Could not retrieve the Recovery Manager for Exchange install location from the registry. Check the Recovery Manager for Exchange installation.	The install location for Recovery Manager for Exchange could not be retrieved from the registry. ■ Check that you have access to the registry location for the Recovery Manager application and ensure that the registry value for the repository location exists. ■ To locate the registry key, open Windows Registry using `regedit`. Check for the following key: HKEY_LOCAL_MACHINE\SOFTWARE\3PAR\RM_Exchange.
5157	RME5157: ERROR: Could not open the Recovery Manager for Exchange registry key. Check the Recovery Manager for Exchange installation.	The registry key for Recovery Manager for Exchange could not be opened. ■ Check that you have access to the registry location for the Recovery Manager application and ensure the registry value for repository location exists. ■ To locate the registry key, open Windows Registry using `regedit`. Check for the following key: HKEY_LOCAL_MACHINE\SOFTWARE\3PAR\RM_Exchange.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5158	RME5158: ERROR: Could not retrieve the Recovery Manager for Exchange repository location from registry. Check the Recovery Manager for Exchange installation.	The repository location for Recovery Manager for Exchange could not be retrieved from the registry. ■ Check that you have access to the registry location for the Recovery Manager application and ensure that the registry value for the repository location exists. ■ To locate the registry key, open Windows Registry using `regedit`. Check for the following key: HKEY_LOCAL_MACHINE\SOFTWARE\3PAR\RM_Exchange.
5159	RME5159: ERROR: Maximum number of volumes exceeded.	Microsoft VSS only allows a maximum of 64 volumes to be simultaneously participated in a snapshot process. ■ Reduce the number of volumes for the snapshot
5162	RME5162: ERROR: Unable to get Netbackup install information from registry.	The Netbackup installation information could not be retrieved from the registry. ■ Check that NetBackup is properly installed and make sure you have access to the registry entry. ■ Confirm the Netbackup installation from Add/Remove Programs. ■ Use `regedit` to check for the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5163	RME5163: ERROR: Could not open NetBackup path registry key '<Registry key path>'.	Could not open the Netbackup path for the specified registry key. ■ Check that NetBackup is properly installed and make sure you have access to the registry entry. ■ Confirm the Netbackup installation from Add/Remove Programs. ■ Use `regedit` to check for the registry key.
5166	RME5166: ERROR: Could not retrieve Exchange server information from the Active Directory.	The Exchange server information could not be retrieved from the Active Directory. ■ Check the Active Directory connection. Try opening the Exchange administrative UI or Exchange Console to determine if the connection is active.
5169	RME5169: ERROR: A VSS unexpected error has occurred. It is recommended to wait ten minutes and try again, up to three times.	An unexpected VSS error has occurred. ■ Try waiting ten minutes and try again, up to three times. ■ Check the application and system event logs for VSS errors.
5171	RME5171: ERROR: The Exchange recovery process failed, you will need to do a manual repair of the Exchange databases.	The Exchange database verification has failed. ■ Make sure both systems have the same level of Exchange server package installed. ■ Manually repair the Exchange database if necessary.
5172	RME5172: ERROR: The Exchange recovery process failed '<Storage Group>': You will need to do a manual repair of the Exchange databases.	The Exchange database verification has failed. ■ Make sure both systems have the same level of Exchange server package installed. ■ Manually repair the Exchange database if necessary.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5173	RME5173: ERROR: Failed to identify Recovery Manager for Exchange agent.	The Recovery Manager for Exchange Agent service is not functioning properly. ■ Restart the Recovery Manager for Exchange service from Windows Services and try the operation again.
5174	RME5174: ERROR: The mount point you have provided does not exist.	The specified mount point does not exist. ■ Make sure the mount point being provided already exists on the system.
5182	RME5182: ERROR: Could not open include file <File Path>. Check to see if your policy name is correct.	The specified NetBackup include file could not be opened. ■ Check the NetBackup policy setting; it is case sensitive.
5184	RME5184: ERROR: Failed to unmount from specified mount point.	Could not unmount from the specified mount point. ■ If the mounting status still shows "Mounted", use the `reset` command to reset the mount status.
5185	RME5185: ERROR: Failed to locate snapshot information from provider: <Snapshot Info Path>.	The specified snapshot information could not be located. ■ Check the 3PAR VSS Provider log for more detailed information.
5186	RME5186: ERROR: Could not retrieve value from provider's XML repository to set snapshot volume.	Value required to set the snapshot volume could not be retrieved from the VSS Provider's XML repository. ■ Check the 3PAR VSS Provider log for more detailed information.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5187	RME5187: ERROR: Failed to get Exchange Server install location from registry.	The Exchange Server install location could not be determined from the registry. ■ Make sure the Exchange Server or Exchange Management tool package is installed on the system.
5190	RME5190: ERROR: Failed to confirm data integrity of the Virtual Copy <Timestamp>. Try performing recovery operations and integrity check to fix.	The data integrity of the specified Virtual Copy could not be confirmed. ■ Perform an integrity check on the virtual copy using the Microsoft Exchange utility `eseutils.exe`. Please consult the Microsoft Exchange documentation for details on how to use this utility.
5191	RME5191: ERROR: Virtual Volume <Virtual Volume Name> is currently exposed to host(s).	The specified Virtual Volume is currently exposed to a host. ■ Make sure the Virtual Copy is not exposed to other hosts from the InServ.
5194	RME5194: ERROR: Invalid backup component document path to import Virtual Copies.	The backup document generated during the Virtual Copy creation is corrupted.
5195	RME5195: ERROR: Failed to perform remote copy command for group <Remote Copy Group Name>.	The remote copy command for the specified group could not be performed. ■ Check the Remote Copy connection and InServ setup. Consult the 3PAR InForm OS CLI Administrators Manual or the 3PAR InForm OS Management Console Online Help for details on setting up and checking remote copy functionality.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5196	RME5196: ERROR: Failed to query remote copy registered volumes information.	Could not query the remote copy registered volumes information. ■ Check the Remote Copy connection and InServ setup. Consult the 3PAR InForm OS CLI Administrators Manual or the 3PAR InForm OS Management Console Online Help for details on setting up and checking remote copy functionality.
5198	RME5198: ERROR: Unexpected remote copy status: <Status Code> for group <Remote Copy Group Name>.	An unexpected remote copy status code has been generated for the specified group. ■ Check the Remote Copy connection and InServ setup. Consult the 3PAR InForm OS CLI Administrators Manual or the 3PAR InForm OS Management Console Online Help for details on setting up and checking remote copy functionality.
5199	RME5199: ERROR: Remote copy group <Remote Copy Group Name> is not found.	The specified remote copy group could not be located. ■ Check the Remote Copy connection and InServ setup. Consult the 3PAR InForm OS CLI Administrators Manual or the 3PAR InForm OS Management Console Online Help for details on setting up and checking remote copy functionality.

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5212	RME5212: ERROR: Failed to cleanup previously created snapshot for remote copy.	A previously created snapshot could not be cleaned up for the remote copy procedure. ■ Manually remove the snapshot from the InServ. ■ Use `rmexch analyze` to determine which snapshots are on the InServ but not reflected in the RME repository. Use `removevv` (and if required `removevlun`) to remove the unwanted VVs. See Chapter B, *Troubleshooting* for more details.
5213	RME5213: ERROR: Failed to send notification command for remote copy.	The notification command was not sent for Remote Copy. ■ Check the communications between your system and the target system using `ping`. You may also need to check the firewall settings.
5215	RME5215: ERROR: Exception occurred during remote copy process.	An exception error occurred during the Remote Copy process. ■ Run `RMReport` to send the information to 3PAR support.
5219	RME5219: ERROR: Failed to set mount point for volume.	The mount point for the volume could not be set. ■ Make sure the mount point exists and is not being used by another application.
5403	RME5403:ERROR: Unable to find the specified storage group '<group name>' in Active Directory.	The specified storage group name could not be located in the Active Directory. ■ This error occurs when attempting to remove or mount a Virtual Copy when the storage group has already been removed or updated from the Exchange server.

3PAR Confidential

Table C-1. Recovery Manager for Microsoft Exchange Event Messages *(continued)*

Event ID	Error Message	Description/Action
5408	RME5408: ERROR: Remote Copy is not ready for sync.	Remote Copy cannot initiate the sync operation. ■ Check that the Remote copy group is in a "Synced" state, using the InServ `showrcopy` command. (Refer to the 3PAR InForm OS CLI Administrator's Manual for details.) ■ Use `ProvCfg` to check that the primary InServ is configured as default on the primary production server. (For ProvCfg.exe utility details, refer to the Provider's user's guide.)
5412	RME5412: ERROR: Unable to locate remote copy group.	The remote RC group could not be located. ■ Use `ProvCfg` to check that the target InServ is configured as default for the remote backup server. (For ProvCfg.exe utility details, refer to the Provider's user's guide.)
5414	RME5414: ERROR: Virtual copy verification failed.	The Virtual Copy verification has failed. ■ Try to verify the virtual copy using the `RMExch validate` command.

3PAR Confidential

Index

A

advisories 1.5
audience for this guide 1.1

B

backup
  full 8.3

C

cautions, defined 1.5
checkpoint file 8.2
circular logging 8.2
configuring
  host computer and controller nodes 4.2
  the database 4.2
controller nodes and host computer,
    configuring 4.2
conventions
  typographical 1.4

D

database
  configuring 4.2
database file 8.2
database recovery 8.4
  point-in-time 8.4
  point-of-failure 8.8
  single mailbox recovery 8.9
database, configuring 4.2
documents, related 1.2

E

Exchange 2007
  file types 8.2
Exchange database
  making changes to 8.2

F

file type
  checkpoint 8.2
  database 8.2
  facilitating database management 8.2
  log 8.2
  optimizing performance 8.2
  patch 8.2
full backup 8.3

G

GUI
  menu bar 6.3
  node tree pane 6.4
  right pane 6.4

H

host computer and controller nodes,
    configuring 4.2

3PAR Confidential

I

installation location of Recovery Manager 4.2
installation of Recovery Manager, verifying 3.5
installing Recovery Manager 3.3

L

log file 8.2

M

menu bar 6.3
Microsoft Volume Shadow Copy Service (VSS) 2.4
Microsoft VSS 2.4

N

node tree pane 6.4
notes, defined 1.5

O

organization of this guide 1.3

P

patch file 8.2
point-in-time recovery 8.4
point-of-failure recovery 8.8
policy setting 6.6

R

recovery
  database 8.4
Recovery Manager
  commands 7.3
  default installation location 4.2
  installation 3.3
  policy setting 6.6
  verifying installation 3.5
related documents 1.2
Remote Copy 9.1, 9.2
  setting up 9.3
revision history RH.1
right pane 6.4

S

search path 4.2
server maintenace
  required tools B.2, C.11
server maintenance
  required tools A.2
setting Recovery Manager policies 6.6
setting up Remote Copy 9.3
setting virtual copy limit 6.7
single mailbox recovery 8.9
storage group
  recovering from a secondary site 9.3
streaming file
  file type
    streaming 8.2

T

Troubleshooting
  troubleshooting B.2
typographical conventions 1.4

U

understanding the registry, registry 3.5

V

verifying installation of Recovery Manager 3.5
virtual copies
  advantages to using 8.3
  explanation of 8.3
virtual copy
  as a scheduled task 7.35
VSS 2.4

W

warnings, defined 1.5
Windows scheduled tasks 7.35

3PAR Confidential

Revision History

Release level	Revision summary
320-200245 Rev A September 2010	First release of this document for version 4.1.0.