Abstract

This white paper discusses how Replication Manager offers an end-to-end solution to a continuous availability of Microsoft Exchange using different replication technology.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>4</td>
</tr>
<tr>
<td>Replication Manager Product Family</td>
<td>4</td>
</tr>
<tr>
<td>Replication Manager/Local</td>
<td>4</td>
</tr>
<tr>
<td>Replication Manager/Remote</td>
<td>4</td>
</tr>
<tr>
<td>Replication Manager/SE</td>
<td>4</td>
</tr>
<tr>
<td>Microsoft Framework Integration</td>
<td>4</td>
</tr>
<tr>
<td>Volume Shadow Copy Service</td>
<td>4</td>
</tr>
<tr>
<td>CLARiiON Replication Methods</td>
<td>5</td>
</tr>
<tr>
<td>Symmetrix Replication Methods</td>
<td>6</td>
</tr>
<tr>
<td>Replication Manager/Local Architecture</td>
<td>7</td>
</tr>
<tr>
<td>Replication Manager Console</td>
<td>8</td>
</tr>
<tr>
<td>Replication Manager Server</td>
<td>8</td>
</tr>
<tr>
<td>Replication Manager Exchange Clients</td>
<td>9</td>
</tr>
<tr>
<td>Exchange Production Server Configuration</td>
<td>9</td>
</tr>
<tr>
<td>Disable Circular Logging</td>
<td>9</td>
</tr>
<tr>
<td>CLARiiON Recommendations</td>
<td>10</td>
</tr>
<tr>
<td>Other Recommendations</td>
<td>10</td>
</tr>
<tr>
<td>Exchange Backup Server Configuration</td>
<td>10</td>
</tr>
<tr>
<td>Microsoft Exchange 5.5/2000 Replication Process</td>
<td>10</td>
</tr>
<tr>
<td>Microsoft Exchange 2003 Replication Process</td>
<td>11</td>
</tr>
<tr>
<td>Restore Exchange Replicas</td>
<td>11</td>
</tr>
<tr>
<td>Restore Considerations</td>
<td>12</td>
</tr>
<tr>
<td>Exchange Mailbox Store Recovery</td>
<td>12</td>
</tr>
<tr>
<td>User Mailbox Recovery</td>
<td>13</td>
</tr>
<tr>
<td>Recovering a Deleted Mailbox Using Exchange System Manager</td>
<td>13</td>
</tr>
<tr>
<td>Reconnecting a Deleted Mailbox to a New User Object</td>
<td>14</td>
</tr>
<tr>
<td>Recovering a Deleted Mailbox Using Exchange Recovery Storage Group</td>
<td>15</td>
</tr>
<tr>
<td>Additional References</td>
<td>20</td>
</tr>
</tbody>
</table>
Overview

Replication Manager is a family of products that simplifies, automates, and manages the creation of disk-based replicas. Point-in-time copies of your mission-critical data are created and managed seamlessly via a user-friendly interface. Numerous benefits are offered with disk-based replication versus traditional backup and data protection schemes. This paper outlines the methodologies Replication Manager/Local uses to create these replicas and the benefits they provide.

Replication Manager Product Family

The Replication Manager product family consists of three distinct offerings, Replication Manager /Local, Replication Manager /Remote, and Replication Manager /SE. The following sections provide a brief description of each product’s features.

Replication Manager/Local

Formerly known as EMC® Replication Manager or ERM, Replication Manager/Local creates application-focused or file-system replicas within a single storage array. Replica creation, access, and retention are easily managed via a graphical interface that can be installed on the desktop to facilitate remote management. Replication Manager/Local provides support for a wide variety of UNIX-based operating systems, Microsoft Windows, and a large assortment of applications.

Replication Manager/Remote

Replication Manager/Remote, formerly known as Storage Data Mobility Manager or SDMM, creates replicas between multiple Symmetrix® arrays providing disaster recovery and restart. Leveraging SRDF® features and functionality, it provides multiple source and target configuration combinations. Remote management of the SDMM server is provided via a SDMM client interface.

Replication Manager/SE

Replication Manager/SE, also referred to as RM/SE in the remainder of this document, is the newest addition to the Replication Manager family. Replication Manager/SE provides support for replica creation on Microsoft Windows platforms attached to CLARiiON® arrays. Replication can be local via SnapView™ or remote between arrays with SAN Copy™. RM/SE was designed to address the needs of a specific market segment, entry level or commercial space Microsoft Windows and application (SQL and Exchange) user environments.

Microsoft Framework Integration

Replication Manager/Local leverages the functionality provided by Microsoft that facilitates the creation of application integrated snapshot backups. Specifically, Replication Manager/Local provides support for Exchange 2003 snapshots via Volume Shadow Copy Service (VSS).

Volume Shadow Copy Service

The Volume Shadow Copy Service, also known as VSS, provides the framework to create point-in-time, transportable backups of Exchange 2003 with snapshot (clone or copy-on-write) backups. There are three components of VSS: a requestor, a writer, and a provider. A VSS requestor is typically a backup application—it requests shadow copy set. Replication Manager /Local is a VSS requestor. The VSS writer is the application-specific logic needed in the snapshot creation and restore/recovery process. The VSS writer is provided by Exchange 2003 and other applications. The VSS provider is third-party hardware control software that actually creates the shadow copy. EMC has providers for both CLARiiON and
Symmetrix systems. The Volume Shadow Copy Service coordinates these component’s functions shown in Figure 1.

VSS provides point-in-time recovery and roll-forward recovery via Copy and Full backup mode. Both modes back up the databases and transaction logs, but only Full mode truncates the logs after successful backup. Since these snapshots are transportable, they can also be used for repurposing. For instance, if your server is attached to a storage area network (SAN), you can mask the shadow copy from the production server and unmask to another server that can reuse it for backup or mailbox-level recovery.

![Figure 1. Volume Shadow Copy Service Components](image)

**CLARiiON Replication Methods**

On the CLARiiON arrays, Replication Manager /Local can take advantage of both clone and snapshot functionality. When you create a replica using clone functionality, you make an exact copy of the data onto a separate logical unit (LUN) or disk. When you create a snapshot replica, the data is stored as a copy on first write to disk-based cache memory. Snapshots only store the information from changed tracks, so they use a minimum of cache storage space on the CLARiiON array. Clones should be used for long-term storage or storage of more critical data, while snapshot replicas can be used effectively for short-term data storage and working copies of the data. Another storage option that Replication Manager /Local supports is the CLARiiON CX series with low-cost Advanced Technology-Attached (ATA) disks. These devices can reduce the cost per megabyte of the storage, and therefore reduce your overall storage investment. ATA disks should also be used for long-term retention of replicas.

SnapView clone replicas are full, exact copies of production data created using SnapView clones. Since they are complete copies of source LUNs, clones can be an effective means of storing critical data for long durations. A clone LUN must be the exact size of the production LUN.

SnapView snapshots are virtual point-in-time copies of a LUN. Snapshots are comprised of data that resides on the source LUN and on the snapshot cache. The data on the snapshot cache consists of copies of the original source LUN data that have been modified since you started the session. During a snapshot session, the production host is still able to write to the source LUN and modify data. When this occurs, the software stores a copy of the original data in the snapshot cache. This operation is referred to as copy on first write and occurs only once for each chunk of data that is modified on the source LUN.

SAN Copy is a storage-system-based Data Mover application that uses a SAN to copy data between storage arrays (Symmetrix-to-CLARiiON and CLARiiON-to-CLARiiON). A snapshot of the production LUN is
used as the source, and a full copy of the data is copied via the SAN to the target LUN on the remote CLARiiON array.

Depending on your application needs, you can create clones, snapshots, or a combination of both. In general, you should use clones for large amounts of data that change frequently, and snaps for data that is more static. Clones always require the same amount of disk space as the source LUN. Snapshots, on the other hand, only require enough snapshot cache space to support the data that has changed on the source LUN (typically 10 to 20 percent of the source LUN size, but will vary depending on how much data has changed). Also, clones typically take longer to create than snaps. However, snapshots may have a bigger impact on performance due to the amount of potential data copies required to synchronize the snapshot cache. This is especially true for source data that changes frequently. Note that Microsoft does not recommend using snaps for Exchange replicas. Doing so may impact the performance of the production databases.

**Symmetrix Replication Methods**

The Symmetrix array offers the highest security and availability for your most critical data applications. Replication Manager can create replicas on business continuance volumes (BCVs) using TimeFinder®/Mirror or on virtual devices (VDEVs) for Symmetrix DMX™ using TimeFinder/Snaps. When you create a replica using BCV technology, you are creating an exact copy of the data by synchronizing and splitting a BCV. When you create a replica using VDEVs for Symmetrix DMX, Replication Manager /Local uses space-saving, pointer-based (copy on first write) snapshots of your production volumes to create the replica. BCVs should be used for long-term storage of your most critical production data, while VDEVs can be used for short-term storage and working copies of the same critical data.

TimeFinder/Mirror creates BCVs, which are mirror images of active production volumes that are point-in-time copies of production data stored in the Symmetrix system. EMC TimeFinder/Mirror provides the mirror establish, split, and restore capabilities that the Replication Manager needs when storing data on the Symmetrix system.

TimeFinder/_snap operations provide instant snap device copies, using VDEVs. A VDEV is a host-accessible device containing track-level location information (pointers) that indicates where the copy session data is located in the physical storage. VDEVs consume minimal physical disk storage, as they store only the address pointers to the data stored on the source device or a pool of save devices. When a virtual copy session is activated, a point-in-time copy of the source device is immediately available to its host via the corresponding virtual device. Upon a first write to the source device during the copy session, a preupdated image of the changed track will be copied to a save device. The track pointer on the VDEV will then be updated to point to the data on the save device.
Replication Manager/Local Architecture

Replication Manager/Local uses the LAN and SAN to communicate and control storage-based functions. Figure 2 shows the Replication Manager architecture and the components that reside in various parts of the system.

Figure 2. Replication Manager Architectural Overview
**Replication Manager Console**

The Replication Manager Console lets you control Replication Manager from Windows or UNIX workstations that have the console installed and have a TCP/IP connection to the RM/Local Server. The console is a portable Java application that communicates with the Replication Manager server, over standard TCP/IP sockets.

![Replication Manager Console](image)

**Figure 3. Replication Manager/Local User Interface**

**Replication Manager Server**

The server software is installed on the server that controls replication activities and stores data about each replica. The server software has three distinct components:

- The Replication Manager server daemon controls and coordinates replication and recovery activity for all the storage corresponding to its registered clients and their InfoSets. The IRD also handles all requests from the Replication Manager Console.

- The policy engine links Replication Manager with the supported storage arrays (for example, CLARiiON). The policy engine is a dynamic library that links to the Replication Manager daemon or service.

- The Replication Manager repository is an embedded database that stores data about InfoSets (Exchange Storage Groups information), activities (mount, backup, log truncation, etc.), and replicas.
Replication Manager Exchange Clients

The client software is installed on each Exchange server that participates in the replication process, including hosts that manage production data and hosts that are used as Exchange standby or backup servers. The client software also has three distinct components:

- **Client control process** — This component communicates with the Replication Manager daemon and sends commands to the other components in this section to perform discovery, database freeze, database thaw, and various storage tasks. This component also returns application files to the daemon to be stored in the database after the replica has been created.

- **The Replication Manager application Exchange agent** — This component communicates with the Microsoft Exchange database to discover storage group information and issue commands such as freeze and thaw using the Exchange 2003 VSS Writer at the appropriate times when a replica is being created. Each agent provides Replication Manager with a logical view of the data that resides on the storage array. Based on this view, Replication Manager can:
  - Specify which storage groups to replicate.
  - Ensure that the data can be replicated safely.
  - Return the database to normal operation.
  - Dismount mailbox stores during restore operations.

- **Storage services** — This component also resides on the client and manages the storage relationships between the client and the storage technologies used to create the replicas. It also discovers information about the storage systems, and issues commands to split (or fracture) mirrors when appropriate to create a replica.

Exchange Production Server Configuration

Planning your implementation is essential. Consult the *Replication Manager /Local Administration Guide* for detailed installation instructions, requirements, and limitations. For instance, data that is shared in a Microsoft Cluster Service (MSCS) environment will require an alternate, nonclustered mount host, as Microsoft does not support mounting replicas of MSCS disk onto a clustered host. Ensure that you have met the prerequisite software and hardware requirements as outlined in the Release Notes and *Replication Manager /Local Software Matrix*.

Because the database replication process takes place transparently to the Exchange server, there are minimal requirements on the server itself. All Exchange database and log files to be backed up must be on Symmetrix or CLARiiON storage. You can use the Exchange System Manager to relocate all of the Exchange databases and logs to the appropriate volumes. This includes all database files (*edb* and *.stm*) and the Information Store transaction logs for each Exchange storage group. Note Replication Manager supports all RAID types. CLARiiON concatenated LUNs are also supported.

It is also best to arrange the data so that volumes used for Exchange data do not share physical volumes with other data that is not associated with that storage group. This prevents potential problems when you restore data from a replica to the production Exchange server.

The checkpoint file (*E00.chk*) for each Exchange storage group must be located on the Symmetrix or CLARiiON LUN holding the logs for that storage group.

Disable Circular Logging

Circular logging is disabled by default after an Exchange 2000 installation. If you have turned on circular logging, you must disable it for proper Exchange recoverability after a hot-split backup. Circular logging alleviates storage constraints on the transaction log volume by keeping only the latest five logs and deleting the rest. Without a full history of transaction logs, you cannot replay transactions against a cloned copy of the Information Store. When circular logging is disabled, you must be more careful with log file maintenance. Transaction logs continue to build up until you clean them out by running a hot-split backup or an Exchange online backup. Properly configure deleted item retention. Microsoft Exchange Server
allows you to retain deleted items for a specified period. You can restrict the purging of these deleted items after a full backup. If you select this option, be sure to run periodic standard Exchange online backups. CLARiiON hot-split backups do not purge these deleted items.

**CLARiiON Recommendations**

For best performance, and to best maintain file-level consistency, you must configure your LUN partitions to begin on byte boundaries that are divisible by 64 kilobytes (KB), matching the default CLARiiON element size. EMC recommends using the Microsoft diskpar utility to do this when you create a LUN.

To increase performance of your Exchange server, follow these recommendations:

- Create the database LUNs as RAID 5 or RAID 1/0. (RAID 1/0 is particularly advisable for environments with higher-than-average write ratios.)
- Create the log file LUNs as RAID 1 or RAID 1/0.
- Move the SMTP queue away from the system volume and onto a CLARiiON LUN formatted as RAID 1 or RAID 1/0.

**Other Recommendations**

If you want to restore at the storage-group level, Microsoft Exchange 2000/2003 storage groups must be arranged on physical volumes so that each storage group uses separate physical volumes for the Exchange data and the logs.

If you want to restore individual mailbox stores, each store must be located on a separate physical volume.

**Exchange Backup Server Configuration**

To mount the Exchange replica for consistency checking only, it is not necessary to install the complete Exchange server software on the backup host. You need to copy only the appropriate Exchange consistency checking utility to the backup host. For Exchange 2000/2003, copy eseutil.exe and ese.dll from the production Exchange server to the mount host and specify that location in the Replication Manager activity.

**Microsoft Exchange 5.5/2000 Replication Process**

Replication Manager automatically creates a physical copy of the Exchange databases (Information Store) and transaction log files for the storage groups that you select. Replication Manager uses the instant-split capabilities to manage the actual replica creation. Instant-split technology divides the process into two phases: a foreground split and a background split. Instant split is the mirror split process that can make a clone or BCV available as a point-in-time copy of the mirrored data almost immediately. Replication Manager completes the foreground split almost instantly and returns a success status to the production Exchange server. At the same time, the background split continues to split the mirror until the split is complete. If the production Exchange server tries to access information on a track that has not been split, the system first splits the track and then completes the I/O request. The following steps illustrate the Microsoft Exchange 2000 hot-split replication process:

1. Check the Exchange Server event log for database consistency errors. As Exchange reads pages in its databases, it checks them for damage (referred to as a torn page), and reports them in the event log as a -1018 error. The database can usually continue running, but you should perform a recovery as soon as possible. Replication Manager checks the event log for -1018, -1019, and -1022 errors and stops upon finding a torn page. This helps to avoid synchronizing a corrupted database on top of your previous good replica.

2. Extract the database and log paths from the production Exchange server.
3. Establish the mirrors (or create the snapshot sessions) and create a replica that captures the data, logs, and the Microsoft Exchange checkpoint files for the selected storage groups.

4. Create the replica by performing an instant split.

5. Mount the replica to backup server. In a CLARiiON environment, Access Logix™ is automatically used to present the LUNs to the backup server. There is no need to present the LUNs manually ahead of time.

6. Check the database consistency using esetutil (esefile in the case of Exchange 5.5). When you run an integrity check on the database replicas, you can expect to find a logical inconsistency reported because the replica has been split while the database was active. Upon recovery, log files are applied to make the database current and consistent. The integrity check looks for evidence of physical inconsistencies and damaged database pages, which are indicated by a checksum error. The Exchange esetutil utility looks for checksum errors in Exchange 2000 databases. When the utility reports no checksum errors, the database is available for recovery.

7. Truncate Exchange logs using Exchange backup API.

The production Exchange server remains available throughout the entire replication. There is no disruption of the production Exchange server during this process.

**Microsoft Exchange 2003 Replication Process**

If you are creating replicas of Exchange 2003 you will not use hot-split technology to quiesce the Mailbox Stores. Instead, Replication Manager uses VSS to perform a truly online replication. In this environment, you can select Full or Copy as the replication option:

- **Full** — Replication Manager replicates the storage group(s), transaction logs, and checkpoint files, and then runs esetutil to verify the consistency of the databases. If esetutil completes successfully, Replication Manager instructs the Exchange VSS Writer to truncate the logs so that only changes that are uncommitted to the database remain.

- **Copy** — Replication Manager replicates the storage group(s), transaction logs, and checkpoint files in the same way as it does during a Full option; however, it does not truncate the logs. Copy replications are often intended for testing and diagnostic purposes only.

A limitation in the Microsoft’s Exchange VSS Writer prevents two Exchange 2003 replicas from running at the same time on the same machine, even if they are replicating different storage groups. Therefore, Replication Manager runs one replica at a time; subsequent replicas must wait until the previous replica is completed.

**Restore Exchange Replicas**

There are a couple of different scenarios and methods for performing Exchange recoveries. You may need to recover a server due to corruption or perform a mailbox restore. Depending on the circumstance and the version of Exchange being recovered, the processes will vary. Refer to the Microsoft *Exchange Disaster Recovery Guide* for your specific version of Exchange. This guide provides details on each of the possible recovery methods.

Replication Manager can manage either a partial (database only) or full (database and log) restore of Exchange replicas to the production Exchange server. Replication Manager dismounts the Exchange databases in the storage group that is being restored prior to the restore operation. The recovery operation will leave the stores dismounted. This is done purposely to allow the user to perform administrative tasks.

When a Microsoft Exchange replica is restored, any of the following restore options can be chosen:

- All storage groups in the InfoSet
- One or more storage groups in the InfoSet
- One or more database(s) from the InfoSet (database files only or database files and log files)

When an Exchange database is restored, the restored files include a checkpoint file (.chk). This file records the location of the transaction log files of the last complete transaction that the Exchange Extensible Storage Engine (ESE) wrote to the database. If a full restore of databases and log files is performed, the checkpoint file enables Exchange to know where to start if the database is rolled forward. If the checkpoint file isn’t present or has been deleted, Exchange begins with the oldest transaction in the log files. If a partial restore of an Exchange database is performed without restoring the log files, Microsoft recommends that the .chk file be removed from the system path folder after the restore but before application of the logs.

**Restore Considerations**

If a replica contains one storage group and both logs and databases are selected for restore, the logs will overwrite any newer logs created since the replica was created. This means that the database will represent the point in time when the replica was taken. To preserve logs created since the replica was taken, only the database(s) should be restored without transaction log files. This will prevent Replication Manager from restoring older logs over newer logs.

To restore at the storage-group level, Exchange storage groups must be arranged on Symmetrix volumes so that each storage group uses separate physical volumes for the Exchange data and the logs. To restore individual databases, each database must be stored on a separate physical volume.

If data other than that associated with the storage group resides on the same physical volumes, users may inadvertently restore data that they did not intend to restore or overwrite data they did not intend to overwrite.

**Exchange Mailbox Store Recovery**

From the Replication Manager User Interface window, expand the replicas object tree, select the replica you want to recover, and invoke the restore wizard. To restore all the datafiles from all the databases in a storage group, without restoring the log files, select **Exchange Database Files** under the selected storage group, as shown in Figure 4.

![Figure 4. Selecting a Mailbox Store from a Storage Group without the Log Files](image-url)
User Mailbox Recovery

One of the most time-intensive tasks for Exchange administrators involves recovering single mailboxes or single messages from Exchange backups. The alternative is a lengthy process of setting up a recovery server, loading the last full backup from tape, and then recovering a single mailbox. Having a standby recovery server saves some time, but adds cost and administrative overhead. To improve service to internal clients and meet Service Level Agreements (SLAs), administrators need a simpler, faster, more accurate method of restoring individual Exchange items. The scenario presented in the next section uses a feature of Exchange to recover a deleted mailbox. The scenario in Recovering a Deleted Mailbox Using Exchange Recovery Storage Group on page 15 recovers a mailbox using Exchange 2003 recovery storage group.

Recovering a Deleted Mailbox Using Exchange System Manager

If you mistakenly delete a mail-enabled user account, you can re-create that user object and then, by default, reconnect that mailbox for a period of 30 days. This is because when you delete a user, Exchange retains a user’s mailbox for a specified period.

You configure Exchange to retain a user’s mailbox in the same way that you specify how many days Exchange retains mail that a user deletes. You configure a deleted mailbox retention period at the Mailbox Store object level.

To configure a deleted mailbox retention period:

1. Using Exchange System Manager, navigate to the Mailbox Store for which you want to configure a deleted-mailbox retention period.

2. Right-click that mailbox store, and select Properties.

The Mailbox Store Properties dialog box appears (Figure 5).

![Mailbox Store Properties, Limits Tab](image)

Figure 5. Mailbox Store Properties, Limits Tab
3. On the **Limits** tab, in the **Keep deleted mailboxes for (days)** field, type the number of days you want Exchange to retain deleted mailboxes.

**Reconnecting a Deleted Mailbox to a New User Object**

If you delete a user account, the user’s mailbox is not actually deleted until the deleted-mailbox retention period expires. The following procedure outlines the steps for reconnecting a mailbox. In the following example, John Doe is a mailbox-enabled user that you previously deleted, and you are within the 30-day deleted mailbox retention period.

To reconnect a deleted mailbox to a new user object:

1. From Active Directory Users and Computers, create a new user object for John Doe.

   **Important:** When creating the new user object, clear the **Create an Exchange Mailbox** checkbox. This is to create a new Windows account without creating a corresponding Exchange mailbox. You will connect this user account to a mailbox later in this procedure.

2. From Exchange System Manager, navigate to the Information Store on which John Doe’s mailbox is located. In the details pane, locate the mailbox for John Doe.

   **Note:** Verify that the **Mailbox** icon appears with a red X, as shown in Figure 6. Mailboxes that are displayed with a red X are mailboxes that have been deleted but will be retained in the mailbox store until the deleted mailbox retention period expires. If the **Mailbox** icon does not appear with a red X, right-click **Mailboxes** and select **Run cleanup agent**.

   ![Exchange System Manager](image)

   **Figure 6.**Disconnected Mailbox

3. Right-click the mailbox named John Doe, and select **Reconnect**.

4. In **New User for this Mailbox**, select the new user object you created for John Doe, and then click **OK**.
Recovering a Deleted Mailbox Using Exchange Recovery Storage Group

The recovery storage group feature in Microsoft Exchange Server 2003 allows you to mount a replica of an Exchange Mailbox Store on the same server as the original database (production server), or on any other Exchange server in the same Active Directory. This can be done while the production database is running and serving clients. This capability allows you to recover data from an older copy of the database without disturbing user access to current data. One common recovery scenario is to use the recovery storage group to recover mail from individual mailboxes. Mail can be recovered by copying or merging it from the recovery storage group databases to the active database using the mail merge tool built into the Exchange System Manager.

1. Before you can use a recovery storage group, you must first create it manually. Using Exchange System Manager, right-click the Exchange server where you want to create the recovery storage group and select **New, Recovery Storage Group** (Figure 7). Keep in mind that the Exchange replica cannot be mounted when creating the recovery storage group. Even though the entire replica will be mounted, you do not have to recover every database in the replica.

![Figure 7. Creating a New Recovery Storage Group](image)

The **Recovery Storage Group Properties** dialog appears, as shown next.
2. Modify the **Transaction log location** and **System path location** fields to point to where the log files will be mounted. Click OK.

The recovery storage group is created and now you need to add the databases you want to recover.

3. Right-click on the new recovery storage group and select **Add database to recover**.

The **Select database to recover** dialog box appears, as shown next.
4. Select one of the databases that you want to recover and click **OK**.

The properties dialog box for the database appears (Figure 10).

---

**Figure 9. Add Database to Recover**

**Figure 10. Database Properties**
5. Modify the Exchange database and Exchange streaming database fields on the Database tab to point to where the database files will be mounted. Make sure the databases in the recovery storage group are dismounted and This database can be overwritten by a restore option is selected. Then click OK.

6. Using Replication Manager, select the replica from which you want to recover data. Right-click the replica and select Mount Replica. Select the production host and the mount point used when you created your recovery storage group.

![Figure 11. Mount Replica](image)

7. When the replica is successfully mounted, you must change the prefix of the log and system files. Open a command prompt window and change to the directory where the log files are mounted. Run the following command:

![Figure 12. Renaming the Log and System Files](image)

8. Using eseutil, perform a soft recovery of the database using the alternate mount paths of the database, system, and log files. It is important to run the command without any spaces after the /L, /S, and /D options (Figure 13). If the alternate mount path has any spaces in the name, enclose the path in double quotes.
Figure 13. Running eseutil

9. Using the Exchange System Manager, right-click each recovered database in the recovery storage group and select Mount Store. The Database can be overridden by restore option must be selected. Click Yes on the warning dialog box that appears.

10. Once Exchange mounts the databases, you can recover data from mailboxes using the Exchange System Manager. To recover mailbox data, select the Mailboxes node that appears when you expand the database node.

The mailboxes for that database will display in the right-hand panel (Figure 14).

Figure 14. Selecting the Mailboxes Node

11. Select the mailboxes that you want to recover. Right-click and select Exchange Tasks.... The Exchange Task Wizard appears.
12. Click Next.

The Available Tasks window appears (Figure 15).

![Figure 15. Available Tasks Window](image)

13. Select the Recover Mailbox Data option and click Next.

14. Select the appropriate destination Mailbox Store and click Next.

15. Depending on whether you want to merge the mailbox data or copy the mailbox, select to either Merge Data or Copy Data and click Next.

16. Schedule the task and click Next.

17. When you are done recovering mailboxes, use the Exchange System Manager to dismount and delete each database in the recovery storage group. Right-click each database and select Dismount. Then right-click and select Delete.

18. When all of the databases have been deleted, delete the recovery storage group. Right click on the recovery storage group and select Delete.

19. Using the Replication Manager GUI, unmount the replica.

**Additional References**

For more information about Replication Manager/Local, refer to the following sources:

- *Replication Manager Version 2.2 Administrator’s Guide*
- *Replication Manager Version 2.2 Product Guide*
- *Replication Manager Version 2.2 Release Notes*
- *Replication Manager 2.2 Support Matrix*

For more information about Microsoft Exchange 2003, refer to the following source:

- *Using Exchange Server 2003 Recovery Storage Groups*