Exchange DR with Replication Manager/SE

Simplifying Exchange Disaster Recovery on CLARiiON Using SAN Copy and SnapView

Abstract

Replication Manager/SE has capabilities for protecting Exchange Servers from disaster using remote replication capabilities in CLARiiON storage arrays.
Table of Contents

Introduction ................................................................................................................................. 4
  Replication Manager Product Family ................................................................................ 4
  Replication Manager .............................................................................................................. 4
  Replication Manager/SE ....................................................................................................... 4
  Additional Documentation ...................................................................................................... 4
  Assumptions .......................................................................................................................... 4

An Overview of Replication Manager/SE ........................................................................... 5
  RMSE Integration with Microsoft Exchange ........................................................................ 5
  CLARiiON Replication Methods Used by RMSE ................................................................. 5
  Replication Types in RMSE .................................................................................................. 6

Specifics about Exchange Replicas ...................................................................................... 6
  Creating Exchange Replicas .............................................................................................. 6
  Restoring Exchange Replicas ............................................................................................ 9

Disaster Recovery Considerations ......................................................................................... 10

Replication Manager/SE for Exchange Disaster Recovery ............................................... 11
  Exchange DR Using RMSE Full SAN Copy ........................................................................ 11
  Exchange DR Using RMSE Incremental SAN Copy ............................................................ 14
    Impact of Incremental SAN Copy on the Exchange Server ............................................. 15
    Recommendations .......................................................................................................... 15

Conclusion ............................................................................................................................. 17
Introduction
Replication Manager is a family of products that simplifies, automates, and manages the creation of disk-based replicas. These point-in-time copies of mission-critical data have numerous benefits versus traditional backup and data protection. Replication Manager/SE is application-centric, supporting Microsoft Exchange and SQL Server on CLARiiON® arrays. This paper outlines how RMSE can be used to create a solution that provides recovery from localized errors as well as site-wide failures for Microsoft Exchange Servers.

Replication Manager Product Family
The Replication Manager product family consists of Replication Manager (used to be Replication Manager/Local) and Replication Manager/SE. SDMM (used to be called Replication Manager/Remote) is no longer considered a part of the Replication Manager family. A brief description of RM and RMSE follows.

Replication Manager
Replication Manager (RM) creates application-focused or file-system replicas within a single storage array. Replication Manager manages SnapView™ (CLARiiON), TimeFinder® (Symmetrix®) and SAN Copy™ (CLARiiON). Replica creation, access, and retention are easily managed via a graphical interface. Replication Manager supports Exchange, SQL Server, Oracle, and UDP on UNIX and Windows.

Replication Manager/SE
Replication Manager/SE (RMSE) is the latest addition to the Replication Manager family. Replication Manager/SE supports replica creation on Microsoft Windows attached to CLARiiON arrays. Replications can be local via SnapView or remote between arrays with SAN Copy. RM SE was designed for entry-level Microsoft Windows and application (SQL and Exchange) user environments.

Additional Documentation
For more information on Replication Manager, refer to the following publications:

- Replication Manager SE User Guide
- Replication Manager SE Release Notes
- Replication Manager SE Software Support Matrix
- Replication Manager Product Guide
- Replication Manager Administrator’s Guide
- Replication Manager Release Notes

Assumptions
Replication Manager/SE was designed and developed with the application administrator in mind. There is an assumption that the administrator understands backup and recovery techniques as well as disaster recovery techniques for Microsoft Exchange. RMSE uses disk-based replication techniques to create point-in-time consistent copies of Exchange data, which can be used effectively to recover from local corruptions as well as complete site-wide failures. Understanding the management of Exchange Servers is critical to plan, implement, and utilize RMSE.
An Overview of Replication Manager/SE

Replication Manager/SE is a derivative of Replication Manager customized to support Windows-only environments on CLARiiON arrays. A graphical user interface conforming to the Windows style provides a look and feel that is familiar to these users. Replication Manager/SE is designed to put the application administrator in control, and considerable development was made in terms of installation, configuration, and usability to meet the administrators’ needs. Once the storage has been provisioned for the application and its replicas, the administrator is in the driver’s seat. All operational tasks are easily configured via wizard-driven interfaces.

Replication Manager/SE takes advantage of multiple replication capabilities within CLARiiON arrays including SnapView snapshots, SnapView clones, and full and incremental SAN Copy to create local or remote disk-based replicas of Microsoft Exchange and Microsoft SQL Server databases.

RMSE Integration with Microsoft Exchange

Replication Manager/SE supports all of the popular versions of Microsoft Exchange:

- Microsoft Exchange 5.5 on Microsoft Windows 2000
- Microsoft Exchange 2000 on Microsoft Windows 2000

With each of these versions and platforms, Replication Manager uses Microsoft-recommended techniques for discovering application information, quiescing the application, creating snapshots, verifying the validity of the snapshots, truncating log files, and restoring from snapshots.

For example, when replicating, mounting, and restoring Microsoft Exchange 2003 databases on Windows 2003, Replication Manager/SE uses the Volume ShadowCopy Service (VSS) to interact with Microsoft Exchange and with the storage. This creates Exchange replicas that are fully compliant with Microsoft recommendations, and fully supported by Microsoft.

When validating replicas, Replication Manager uses the appropriate Microsoft tools—ESEFILE.EXE for Exchange 5.5, ESEUTIL.EXE for Exchange 2000 and Exchange 2003—to verify the integrity of the replica.

CLARiiON Replication Methods Used by RMSE

Replication Manager/SE uses three different types of CLARiiON replication methods: SnapView clones, SnapView snapshots, and SAN Copy. A brief description of each follows.

SnapView clone replicas are full, exact copies of production data created using SnapView clones. Since they are complete copies of source LUNs (logical units), 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 consist of data that reside on the source LUN and within the snapshot cache. The data in the snapshot cache consists of copies of the original source LUN data that have been modified since starting the snapshot session. During a 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.

Note: When using snapshots for Exchange replication, there is additional overhead on the array associated with copy-on-first-write activity. This can impact the performance of the production environment if it is not configured to handle this extra demand on resources.
SAN Copy is a CLARiiON-based Data Mover application that uses a storage area network (SAN) to copy data between storage arrays. A full SAN Copy session performs a complete block-for-block copy of an entire LUN to a target LUN of the same size or larger. An incremental SAN Copy session keeps track of changes on a LUN since the last copy. Once activated, a snapshot session is started to hold the point-in-time image from which the changed data is copied at the block level to update a target LUN of the same size. When the copy is complete, the target LUN exactly matches the point-in-time image of the source, and the snap session is stopped. SAN Copy is available on some CLARiiON array models.

**Replication Types in RMSE**

Replication Manager/SE performs four types of replications. This section describes the basic replication types and their applicability to Exchange Servers.

- Replications within the same array to snapshots or clone LUNs
  
  The production data LUNs are replicated to either snapshots or clone LUNs within the same array. The validity of the replica is usually verified on another host (mount host) connected to the same array. Clone replicas are an excellent choice for Microsoft Exchange for local recovery. Snap replicas are not generally suitable for Exchange because the ESEUTIL validation taking place on the snapshot results in a significant amount of additional read activity on the production volumes.

- Replications to another array from an existing local replica
  
  An existing, unmounted replica that has already been validated is copied, using full SAN Copy technology, to another CLARiiON array, usually in a different location. Since the source replica for this copy has already been verified, no remote mounting and verification is usually performed. Full SAN Copy replications from existing clones can be a part of a disaster recovery strategy for Exchange Servers, as described later in this paper.

- Full SAN Copy replications to another array from the production data using a temporary snapshot
  
  RMSE creates a snapshot of the production LUNs to be used as the SAN Copy source. Full SAN copy is used to copy this point-in-time image to another CLARiiON array. The verification of the replica is performed on a host attached to the remote CLARiiON array.

  Full SAN Copy replications performed directly from snapshots of the production LUNs do not generally work well with Exchange. The ESEUTIL read activity and SAN Copy activity on the snapshot may compromise production Exchange performance.

- Incremental SAN Copy replication to another array from production data
  
  CLARiiON SAN Copy technology is used to transfer changed data from a snapshot of the production Exchange LUNs to target LUNs in another CLARiiON array. On the remote array, a snapshot is then taken of the target LUN, and this snapshot holds the replica. RMSE running on a remote mount host mounts the snapshot and verifies the transferred replica.

  Incremental SAN Copy replications can be a part of an Exchange disaster recovery strategy, as described later in this paper.

**Specifics about Exchange Replicas**

Replication Manager/SE manages the replication of Exchange data depending on the requirements of the various Exchange versions and the type of replication required.

**Creating Exchange Replicas**

Prior to creating Exchange replicas, some configuration requirements must be met. Information Stores must not reside on the same LUN as their respective transaction logs. The working directory or checkpoint file should be relocated to the same LUN as the transaction logs. Circular logging must be disabled. For

---

1 SAN Copy can also be used to copy data within a single CLARiiON array, but RMSE does not use this functionality.
Exchange 5.5, in addition to the Information Store requirements, the same rules apply to the Directory Store.

Replication Manager/SE can be configured to replicate one or more storage groups (both database and log LUNs) within the Exchange Server. Figure 1 shows the RMSE graphical user interface wizard panel for selecting the storage groups within an Exchange Server for replication.

**Figure 1. Selecting Exchange Storage Groups for Replication**

With Exchange 2003 on Windows 2003, Replication Manager/SE will invoke VSS to create the snapshot. With all other combinations of Windows and Exchange, Replication Manager/SE will perform hot splits, creating a replica and separating it from its source while Exchange is active and unaware.

**Figure 2. Options to Mount and Validate a Replica Using ESEUTIL**

By default, RM/SE will fail the job if any of the following Exchange errors are detected in the event log. Uncheck these errors that you do not want RM/SE to fail for.

- -1016 error (JET Read/Verify Failed)
- -1019 error (JET Page Not Initialized)
- -1022 error (JET Disk I/O Failed)

RM/SE can ignore all the errors that you have selected for the next run of this job. To enable this feature, click Ignore all errors for the next run only.

- Ignore all errors for the next run only

---

Exchange DR with Replication Manager/SE
Simplifying Exchange Disaster Recovery on CLARiiON Using SAN Copy and SnapView
Before starting the replication, RMSE can be configured to scan the Windows Application log for Exchange -10xx errors. The user can configure which errors RMSE should scan for in the logs. This is done purposely to avoid overwriting a good replica with a potentially corrupt copy. Refer to the product guide for additional details.

After the replication process, Replication Manager can be configured to mount the replica to another host, and to verify the integrity of the replica by running ESEUTIL.EXE or ESEFILE.EXE.

**Figure 3. Options to Mount and Validate a Replica Using ESEUTIL**

By default, RMSE will perform an “Online - Full” replication, after which Exchange truncates the committed transaction log files. This keeps the log LUN from getting filled. An “Online - Copy” replication is an option that does not truncate Exchange logs. These and other options selectable through the Replication Options panel are shown in Figure 4.
There are several different scenarios and methods for performing Exchange restores. You may need to restore a server due to corruption, perform a mailbox restore, or repurpose the replica on a test system. The processes will vary greatly depending on the circumstance and the version of Exchange being recovered or reused. Refer to the Microsoft Exchange Disaster Recovery Guide for your specific version of Exchange. This guide provides details on several possible recovery methods.

Replication Manager/SE allows the restore of one or more databases within the Exchange storage groups that were replicated. For recovery with the least amount of data loss, only the database LUNs should be restored. However, RMSE also provides the option to additionally restore log LUNs for a point-in-time recovery. Figure 5 shows a panel used for Exchange Replica Restore within the Replication Manager/SE graphical user interface.
Disaster Recovery Considerations

Disaster recovery deals with planning, deploying, operating, and monitoring a system that will allow continued operation when the primary production site is temporarily or permanently rendered unusable. The most basic requirement for disaster recovery involves making a copy of the production data available at a remote location so that the business operations can be resumed in case of a disaster at the primary production location.

Disaster Recovery has many interrelated considerations such as:

- How frequently copies of the data are created at the remote site
- The format of these copies
- The type of equipment at the remote site

These determine how much data will be lost in the case of a disaster, how quickly the remote site can take over operations after a disaster, and the level of service at the remote site. We will define two basic terms that are used most often in describing the most important aspects of a disaster recovery solution.

**Recovery Point Objective** or **RPO** is a length of time that describes the maximum amount of data loss that would happen if the disaster struck at the most inopportune time. RPO represents the time period for which the updates committed to the production data would be lost when the remote site is started.

For example, if the disaster recovery system counted on weekly backup tapes being created and shipped to a remote location, reliably every Saturday at noon, then the RPO would be seven days. This is because if a disaster were to affect the production site just before Saturday at noon, the remote site would have to restart using a backup that was from Saturday the week before, thus losing seven days worth of updates to the production database.

**Recovery Time Objective** or **RTO** is the length of time that it would take the remote site to be operational after a disaster. RTO is a measure of the length of the outage where the service is unavailable until the remote site comes online.

In the previous example, if it would take three days to set up machines, load software, recover the tape backup, and bring the system online at the remote site, then the RTO is three days.

RTO and RPO are independent. One disaster recovery solution may have a shorter RTO than another, but it may have a longer RPO. In general, disaster recovery solutions that have shorter RTOs and RPOs are more expensive to deploy and operate than those that have longer RTOs and RPOs.

Other considerations for a complete disaster recovery solution include:

- Level of service at the remote site
- Ease of restart at the remote site
- Data protection at the remote site
- Disaster protection at the remote site
- Returning to the original site (or a rebuilt site)

These considerations, while important, are beyond the scope of this paper.
Replication Manager/SE for Exchange Disaster Recovery

Replication Manager/SE can be used to deploy disaster recovery solutions for Exchange Servers with a good RTO and RPO.

There are two basic configurations that are most useful for Exchange DR:

- Full SAN Copy from an existing replica
- Incremental SAN Copy from production data

Both of these configurations create validated point-in-time copies of Exchange databases and logs at a remote location. These copies are periodically refreshed with more current data, while ensuring that at least one recent copy is always present at the remote site.

Replication Manager/SE can create these copies while continuing to create local replications for quick and efficient operational recovery from day-to-day errors, such as accidental deletes and database corruptions.

Exchange DR Using RMSE Full SAN Copy

In this configuration, Replication Manager/SE is set up to create one or more clone replications within the production CLARiiON storage system on a daily schedule. These replicas are mounted to a host attached to the same CLARiiON storage system, and are validated on that host. Then these replicas are unmounted and kept around for the day in case they are needed for rapid recovery from day-to-day errors.

Replication Manager/SE is configured to copy one of these replicas to a remote CLARiiON array using full SAN Copy on a daily schedule. Since the replica was already validated prior to copying, there is no need to mount and run the validation again, although this option is available.

At the remote CLARiiON storage system, two target LUNs are reserved for SAN Copy, and the job is set up to rotate among the two LUNs. This guarantees that there will be at least one good copy available for recovery, even while the next SAN Copy operation is being performed.

Figure 6 illustrates this configuration. Three local clone copies are shown in the figure.
Figure 6. RMSE Full SAN Copy Configuration for Exchange DR

The full SAN Copy configuration is designed to minimize the impact of creating the local and the remote copies on the production Exchange Server. Local copies are created using SnapView Clone technology, which uses independent clone LUNs as targets for the copy. These targets are incrementally synchronized with the productions LUNs. Only the blocks that are different between the production LUNs and the clone LUNs are copied after the first initial copy. Depending on the rate of change of the data, this can be a small fraction of the size of the LUN.

The remote copy is created by performing a full SAN Copy from the clone LUNs to the remote CLARiiON storage system. This does not involve the production LUNs, and so the performance impact on the production server is minimized.
The full SAN Copy configuration does, however, require that the entire Exchange data and log LUNs be copied from the production site to the remote site. The communications link between production site and the remote site must be selected to allow this operation to complete in a reasonable timeframe. Table 1 provides guidelines for various types of communication links, and the amount of data that can be moved in two, four, and eight hours.

Table 1. SAN Copy across Communication Link Types

<table>
<thead>
<tr>
<th>Link Type</th>
<th>Nominal Data Rate</th>
<th>SAN Copy in 2 Hours</th>
<th>SAN Copy in 4 Hours</th>
<th>SAN Copy in 8 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3</td>
<td>45 Mb/s</td>
<td>50 GB</td>
<td>100 GB</td>
<td>200 GB</td>
</tr>
<tr>
<td>OC3</td>
<td>155 Mb/s</td>
<td>180 GB</td>
<td>360 GB</td>
<td>720 GB</td>
</tr>
</tbody>
</table>

The full SAN Copy configuration as described here provides an RPO that is typically greater than 24 hours. The worst-case scenario is where the production site is lost just as the copy is about to complete. The remote site would have to be started from the previous day’s copy. Assuming that the copies are made daily, and the time to perform the ESEUTIL integrity check and complete the copy is 4 hours, 28 hours of updates would be lost.

The RTO of the full SAN Copy DR solution depends on the readiness of the environment at the remote site to assume production operations. The replicas that RMSE moves are verified and in a state ready for the Exchange Server to mount immediately. If the remote site shares the Active Directory environment of the production site and the Exchange Server has already been built to take over the identity of the production Exchange Server, the RTO can be a matter of a few minutes.

---

2 As tested between two CLARiiON CX700 systems through a pair of compressing Nishan bridges. Incremental SAN Copy throughput can differ from full SAN Copy throughput (full SAN Copy uses larger buffers). However, in tests performed for this paper, the throughput was similar for each when the bandwidth was fully utilized—observing a compression ratio of approximately 1.6 to 1.
**Exchange DR Using RMSE Incremental SAN Copy**

In this sample configuration, Replication Manager/SE is set up to create one or more clone replicas within the production CLARiiON array on a daily schedule. These replicas are mounted to a host attached to the same CLARiiON array, and are validated on that host. Then these replicas are unmounted and kept around for the day in case they are needed for rapid recovery from day-to-day errors.

Replication Manager/SE is also configured to perform an incremental SAN Copy from the production Exchange data to the remote CLARiiON storage system on a daily schedule. The job is configured to mount the replicas on a host attached to the remote CLARiiON storage system, and to validate the replica on that host. The job is configured to have a rotation of two replicas.

RMSE will reserve a target LUN in the remote CLARiiON array for each production LUN to be replicated using incremental SAN Copy. In a typical Exchange 2003 job using local replication to clones, RMSE works with VSS to synchronize the clones, split off and protect the replicas, and mount the clones to a local mount host to verify with ESEUTIL. The equivalent process for an incremental SAN Copy job is to create a point-in-time snapshot while Exchange I/O is frozen for a few seconds, copy changed data from the snapshot to the remote site, and mount new snapshots of the SAN Copy targets to a remote mount host for ESEUTIL verification. Multiple replicas can be maintained on these snapshot LUNs.

The incremental SAN Copy job must be scheduled to run at a different time from the local replication job. This is because two jobs cannot be run against the same Exchange Server at the same time.

Figure 7 illustrates this configuration. Three local clone copies and two remote snapshot copies are shown in the figure.

**Figure 7. RMSE Full SAN Copy Configuration for Exchange DR**

The incremental SAN Copy configuration is designed to minimize the amount of data transferred over the communications link. The incremental SAN Copy session within the CLARiiON array keeps track of the changed blocks in the production LUNs, and only transfers the changes when the new replica is created each day. Depending on the amount of change to the database, this can require significantly less communications bandwidth than transferring all of the data every time.
The savings in communication bandwidth, however, comes at the cost of possible performance impact on the production Exchange Server. There is a change-tracking map updated within the CLARiiON array for each of the production LUNs because they are engaged in an incremental SAN Copy session. When the RMSE remote replication job runs, the SAN Copy sessions are marked and activated. This initiates the incremental refresh of the remote target LUNs. While this data movement is in effect, there is additional overhead on the production LUNs. This impact is discussed in detail next.

The RPO of an incremental SAN Copy configuration is determined by how frequently the remote replication job is run plus the time that it takes to complete. If the remote replication job is run every four hours, and takes two hours to complete, the RPO will be six hours.

The RTO of an incremental SAN Copy configuration is determined in a way similar to that for a full SAN Copy configuration. The Exchange replica is transmitted in a state ready to mount and it has already been verified with ESEUTIL. Depending on the point where a site failure occurs, the latest good replica may reside only on the snapshot. In this case you would restore (rollback) the snapshots to the full Exchange LUNs before mounting the LUNs on the production host. At a well-prepared remote site, the RTO can still be as low as a few minutes.

Impact of Incremental SAN Copy on the Exchange Server

When an RMSE incremental SAN Copy job is first run on an Exchange storage group, a new incremental SAN Copy session is created linking the production LUNs for that storage group with matching target LUNs at the remote site. During the period of the run where incremental SAN Copy is actually copying changed data to the remote site, there is an added load on the CLARiiON array. The array must keep a point-in-time image of the production LUNs from the point when RMSE activated the incremental SAN Copy sessions. The array must scan a table to determine which tracks have been changed, read those tracks, and send them over the communications link. It must also maintain the snapshot LUNs that hold the point-in-time images as new write requests are made to the production LUNs (copy on first write). All of these operations can cause an increase in the time required by the array to service read and write requests from the production Exchange Server. The overhead decreases gradually as the copy completes. At all other times when the SAN Copy session is inactive, there is minimal additional overhead (roughly five percent) associated with maintaining the table of changed data blocks for the next cycle.

It is difficult to quantify how much of a performance impact this will exhibit upon the production Exchange Server, and how it will affect users of the Exchange Server. This depends on the configuration and load on the Exchange Server and the CLARiiON array. If the Exchange Server was configured with plenty of headroom in CPU, memory, and other local resources, and the CLARiiON array was configured to handle the additional I/O, the users may not see a degraded response time. If the Exchange Server or CLARiiON array was already near the limit of some critical resources, the additional load from the incremental SAN Copy may cause a significant slowdown in response time to the server.

Recommendations

EMC Engineering has performed tests of a number of Exchange configurations in order to arrive at a set of recommendations. The recommendations are summarized next.

For existing Exchange Servers on CX500 and CX700 storage systems

- If your Exchange Server is currently failing to provide an acceptable response time for your users during peak activity periods, configuring an incremental SAN Copy job will make it worse. You may need to divide the users among two or more Exchange Servers and/or reconfigure your disk usage on the array before deploying this DR solution.
- You should plan incremental SAN Copy jobs to run when the Exchange Server is not at peak loads. Watch the daily behavior to find times when the load tends to be lower—for example, in the morning before a majority of users log on, during lunchtime, or overnight.
- If you find that incremental SAN Copy can run without noticeably impacting users during busy times, you can consider configuring jobs to run more frequently. More frequent runs will reduce the amount...
of changed data needing to be transferred during a particular copy. The minimum RPO possible is a few minutes more than the data transfer time plus ESEUTIL time.

- While running an incremental SAN Copy session, disk response time to the host will increase because of the added number of CLARiiON I/Os associated with a particular host I/O operation—even for an optimally configured array.

- Use the Windows performance monitoring tool (PERFMON) on your Exchange Server. One significant parameter is the RPC Queue Length on the Exchange Server. A queue length under 40 indicates a server with sufficient headroom to run RMSE with incremental SAN Copy. If the queue length is larger than 40, there may not be enough headroom to run incremental SAN Copy, even though the response time seems adequate without SAN Copy.

When the incremental SAN Copy job runs, the RPC queue length can be expected to double. This alone may not show up as a perceptible increase in response time to the users. However, if the queue length nears the limit of 100, there will be an unacceptable increase in response time.

For new to be deployed on CX500 and CX700 storage systems

- Estimate the I/O workload imposed by your Exchange users. Heavy Exchange users represent 0.75 I/Os per second. More typical users average 0.4 I/Os per second. A light user may produce only 0.25 I/Os per second.

- Consider sizing the Exchange Server to support a smaller number of Exchange users than its maximum rating. This increases the likelihood that the Exchange Server and users will be less affected by the slower disk response times during an incremental SAN Copy data transfer.

- Size the CLARiiON arrays according to the number of users, the mailbox sizes, and the replication requirements. More frequent replications and concurrent replications require more system resources. A CX700 system can support from 8,000 to 12,000 average users with replication. A CX500 array can support from 4,000 to 7,000 users.

- The remote CLARiiON storage system should usually be the same model as the local system.

- Size the communication link based on the number of users and the I/O activity. For example, a test of 1,000 users generated roughly 20 GB\(^3\) of change data for incremental SAN Copy in a four-hour period of constant I/O at a rate of .5 to .6 IOPS/user.

- Plan to run the incremental SAN Copy jobs at times of lower load on the Exchange Servers.

For all incremental SAN Copy implementations

- Coordinate the timing of the SAN Copy job to avoid intersecting with a local replication job on the same server.

- If you are also performing local replication to clones with RMSE, set the local job to truncate Exchange transaction logs (for Exchange 2003, this is called Online – Full Replication) and set the SAN Copy job to skip log truncation, the default setting (Exchange 2003 terminology is Online - Copy).

- Avoid running a SAN Copy job during the online maintenance period of the associated databases. One good time to run a job would be shortly after the completion of online maintenance.

---

\(^3\) This number includes both database and log LUNs. It includes all blocks that incremental SAN Copy needed to copy—before any compression, which was seen to be approximately 1.6:1. The read/write ratio was 2:1.
Conclusion

Replication Manager/SE provides automated replication of CLARiiON storage in Microsoft SQL Server and Microsoft Exchange environments.

Replication Manager/SE combines local replication for operational recovery with remote replication for disaster recovery for Microsoft Exchange Server 5.5, 2000, and 2003 environments. All of the replication of Exchange 2003 on Windows 2003 is fully compatible with Microsoft VSS recommendations.

Two different DR configurations for Exchange are supported and recommended—using full SAN Copy technology to create a remote copy from local clone LUNs, and using incremental SAN Copy technology to create a remote replica directly from production LUNs.

Full SAN Copy configurations provide a DR solution with the lowest level of impact on the production environment.

Incremental SAN Copy configurations place more overhead on the production environment. Customers who have environments that can handle this additional overhead should consider this solution’s benefits, which include lower storage and bandwidth requirements, and improved RPO.