White Paper

EMC CLARiiON Guidelines for VMware Site Recovery Manager with EMC MirrorView and Microsoft Exchange

Best Practices Planning

Abstract

This white paper presents guidelines for the use of Microsoft Exchange 2007 on EMC® CLARiiON® as an application protected by VMware Site Recovery Manager and EMC MirrorView™. Factors considered include initial configuration planning, remote recovery, and failback.

June 2009

Part Number h5794.1

Table of Contents

Executive summary

The progressive virtualization of organizations' server environments is taking place at an ever-increasing rate thanks to the considerable cost savings virtualization offers. VMware's Site Recovery Manager (SRM) significantly enhances the ability to provide disaster recovery protection for virtualized environments.

Originally, the Microsoft Exchange server was not a good candidate for virtualization, mostly because of its performance requirements and sensitivities. However with the latest enhancements in Exchange and virtualization software, Exchange is now regularly deployed virtually. This has also been boosted by considerable successful testing and increasing support by Microsoft.

VMware SRM, when combined with EMC replication software, adds a valuable new option for remote protection of an Exchange environment.

Introduction

This white paper addresses the various aspects of working with VMware Site Recovery Manager on an EMC® CLARiiON®. The solution described complies with the Microsoft Server Virtualization Validation Program (SVVP). It is particularly helpful for system architects and administrators who need to design and implement a Microsoft Exchange solution with optimal data protection.

Considerations include:

- Planning and design
- Configuration and implementation
- Optimizing performance and daily administration
- Failover testing
- True failover and remote recovery
- Failback
- Interoperability with Exchange standby continuous replication

Although SRM has been integrated with a range of EMC replication products, this paper focuses on using SRM on CLARiiON systems with MirrorView™ (both synchronous and asynchronous), and describes unique considerations for using this configuration with Exchange. General information for SRM is provided in the *VMware Site Recovery Manager Administration Guide*, and general guidelines for SRM with CLARiiON are provided in the *VMware Site Recovery Manager with EMC CLARiiON CX3 and MirrorView/S Implementation Guide.*

Audience

The intended audience for this white paper is customers — including IT planners, storage architects, and administrators — and EMC technical staff and partners.

The reader should have an understanding of basic Exchange, Windows, VMware, and CLARiiON features and terminology, including MirrorView.

VMware Site Recovery Manager

VMware Site Recovery Manager (SRM) is a disaster recovery framework that integrates with various EMC replication software products (for example, MirrorView for CLARiiON) to automate the failover process of VMware VMFS datastores. SRM recovery plans leverage the array-based snapshot feature to test the failover process and ensure that the secondary image is consistent and usable. SRM relies on independent VMware VirtualCenter servers to be in place at both the protected (primary) site and at the recovery

(secondary) site to facilitate the failover process between the two sites. SRM is made available with a set of storage replication adapters (SRAs). SRA is software that provides the integration with a storage vendor's replication product. The SRA for MirrorView is installed at both sites, onto a machine that has the SRM framework installed. It integrates the CLARiiON mirroring functionality with SRM, supporting array discovery, replicated LUN discovery, test failover, and actual failover.

EMC CLARiiON MirrorView/S

EMC MirrorView/Synchronous is a CLARiiON business continuity solution that provides LUN-level data replication to a remote CLARiiON storage system. The copy of the data on the production CLARiiON array is called the primary image and the copy at the recovery site is called the secondary image. During normal operations, the primary image is online and available for read or write operations, and the secondary image is not exposed. MirrorView/S provides real-time, synchronous mirroring of data between the protected CLARiiON system and the recovery CLARiiON system. With synchronous operations, data must be successfully stored on both the local and remote CLARiiON arrays before an acknowledgment is sent to the local host.

EMC CLARiiON MirrorView/A

EMC MirrorView/Asynchronous is a CLARiiON business continuity solution that provides LUN-level data replication to a remote CLARiiON storage system. The copy of the data on the production CLARiiON array is called the *primary image* and the copy at the recovery site is called the *secondary image*. During normal operations, the primary image is online and available for read or write operations, and the secondary image is not visible to the user. MirrorView/A provides asynchronous mirroring of data between the protected CLARiiON system and the recovery CLARiiON system. With asynchronous operations, MirrorView/A keeps track of changes to the primary image. When an update is triggered, MirrorView/A replicates the changes to the secondary image.

Planning for implementation

Table 1 and Figure 1 describe required optional components in a typical Exchange environment protected with SRM and MirrorView.

Table 1. Virtualized Exchange Infrastructure

Required component	**Description**
Exchange mailbox server(s) within a VMware virtual machine (VM)	Virtual Machine must be running Windows 2003 or Windows 2008 and Exchange 2003 or 2007 (Windows 2008 required for Microsoft SVVP compliance)
EMC CLARiiON storage systems at the protected and recovery sites with MirrorView and SnapView™	Any CX3 (with FLARE® 26 or later) or CX4 model storage system, or a fibre-based AX4-5 system (for more detail see the "CLARiiON model considerations" section)
VMware ESX servers at the protected site and recovery site	Including Virtual Infrastructure (VI) and Site Recovery Manager with the SRA for MirrorView SRM failover protection is available for VMFS datastores. RDMs are not currently supported
Exchange CAS and Hub Transport servers at each site, within the same Windows domain	These may be configured within their own VMs
Optional component	**Description**
Additional ESX servers	Configured with VMware HA to provide local failover protection of the Exchange VMs
Replication Manager servers	As of version 5.1, Replication Manager provides additional protection capability, such as clone or snap-based replicas of the Exchange data at the local site for rapid recovery, and integrated

	backup capability. It also supports clones and snaps of mirrored LUNs at the DR site with MirrorView/S.
EMC SourceOne® (formerly EmailXtender®) servers	To provide legal compliance and to archive Exchange data, resulting in smaller, more manageable backups
EMC Disk Library, DL3D	Storage system functioning as a virtual tape library for rapid, efficient backup of Exchange data disk. Includes capability for high-level deduplication of Exchange data

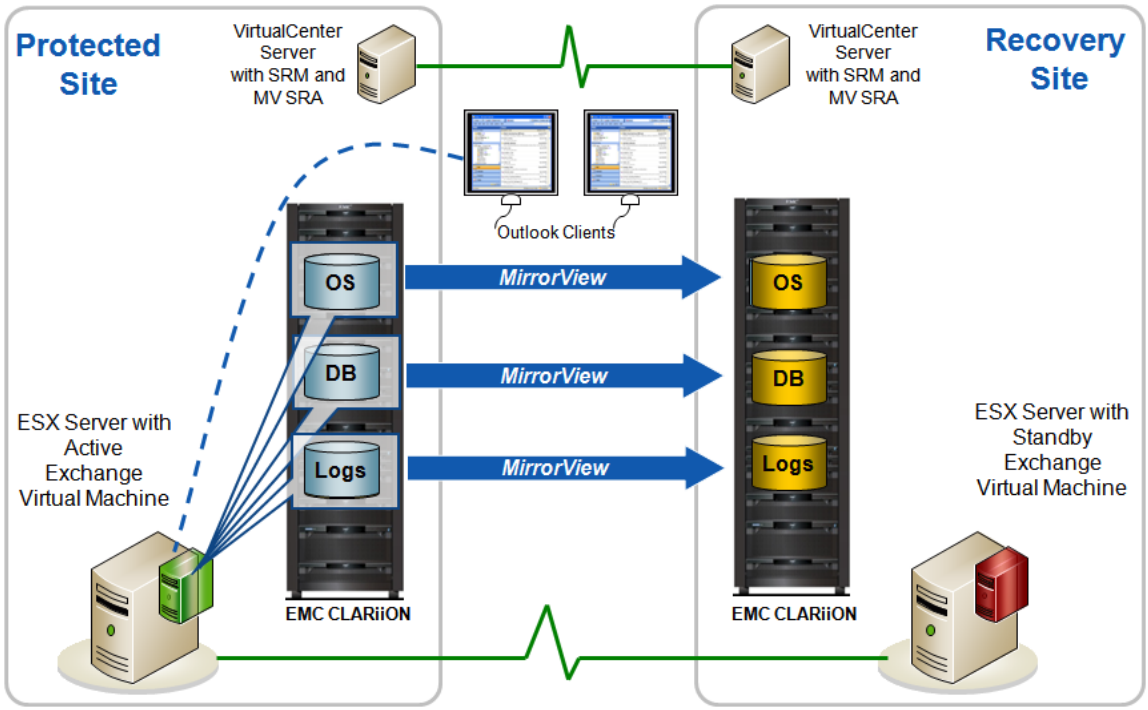

Figure 1. Exchange environment protected by SRM and MirrorView

Array considerations

MirrorView guidelines

This section describes general guidelines for configuring MirrorView in use with SRM and Exchange, followed by specific recommendations for synchronous and asynchronous mirroring.

Latency

With mirroring the I/O response time must still be within the Microsoft guideline limits of:

- 20 milliseconds average for database reads (< 40 ms max)
- 10 milliseconds average for log writes (< 40 ms max)

The link should be tested to confirm that it has sufficient bandwidth and the least possible overhead. Then it should be tested with Exchange to confirm that performance and latency are at acceptable levels.

Write intent log

We recommend the use of the MirrorView write intent log. The write intent log stores a persistent copy of the mirrored writes to hard disk and provides added protection in the event of a power outage or failure of

one of the array's storage processors. It adds a small, usually insignificant, amount of overhead to the mirror. On CLARiiON CX4 models, the write intent log is enabled by default.

Consistency groups

You can place a set of mirrored LUNs into a consistency group when you want to act on the set of LUNs as a unit. For Exchange it is important to place all the LUNs of an Exchange storage group (usually one database LUN and one log LUN) into a consistency group. In this way, any fracture to one of the LUNs in the consistency group will cause a fracture for all LUNs in the consistency group at the same point – allowing the database to remain consistent. *SRM requires that all mirrors it manages be placed in consistency groups.*

The maximum numbers for consistency groups for various CLARiiON models are shown for MirrorView/S in Table 2 and for MirrorView/A in Table 3.

You can place the Exchange LUNs from multiple CLARiiON Storage Groups into the same consistency group. In this case, all mirrored operations (such as fracturing or starting a full synchronization) will take place on the entire set.

NOTE: If you reach the maximum number of mirrors supported in a single consistency group then you can just add another CG. There is no restriction on how many consistency groups can be associated with a VM. Your final configuration will be affected by the limits on mirrors within a CG, and CGs within an array.

Bi-directional mirroring

There is a one-to-one source (primary) / target (secondary) relationship for all mirrors managed with SRM. With MirrorView there can be LUN pairs with mirroring going on in opposite directions, providing bi-directional support where two Exchange production sites can protect each other (see Figure 2).

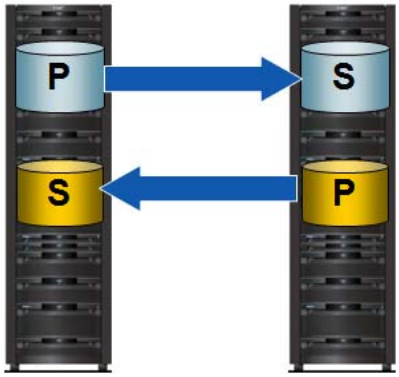

Figure 2. Bi-directional mirroring

It is possible to use SRM and MirrorView to mirror one set of Exchange LUNs to one DR site while mirroring a second set of LUNs on the same array to a different DR site.

Other MirrorView guidelines

- To maximize performance during active periods, avoid taking snapshots of mirrored LUNs (source or target) during these times if possible
- Set the MirrorView recovery policy to **Manual**. This gives you the option to make a copy of the LUNs before performing a full resynchronization as part of a recovery.

MirrorView/S considerations

CLARiiON MirrorView/S provides high-level mirroring of Exchange data with a recovery point objective (RPO) of zero data loss. However, because each local write to the Exchange database is not considered complete until the write to the corresponding remote database has been acknowledged, it is important to consider the added I/O latency of mirroring and how to minimize it.

EMC recommends that for use with Exchange, the distance between the two synchronously mirrored sites is less than 100 km.

MirrorView/A considerations

CLARiiON MirrorView/A provides high-level mirroring of Exchange data with an RPO equivalent to the update frequency plus the time the update takes to finish replicating the changes. For example, if you set MirrorView/A to perform updates once every 30 minutes, and the changes take 15 minutes to replicate, the RPO will be 45 minutes.

As with MirrorView/S, it is important to design to meet the Microsoft Exchange latency guidelines. However, because local write completion is not tied to the remote update, latency can be higher on the remote component. This allows support for considerably higher distances between the two sites. The update frequency your environment can handle will be a function of the network bandwidth between the two sites, the associated network latency, and the change rate of the Exchange data.

CLARiiON model considerations

VMware Site Recovery Manager with MirrorView is supported on the following CLARiiON models:

- AX4-5F
  (MirrorView supported on the fibre model only)
- CX3-10c, CX3-20 and 20c, CX3-40 and 40c, CX3-80
  (iSCSI mirroring requires combo c models and all models require FLARE 26 or later)
- CX4-120, CX4-240, CX4-480, CX4-960
  (iSCSI and fibre-based mirroring)

Table 2. Mirroring limits on CLARiiON storage systems with MirrorView/S

CLARiiON model	Max mirrored pairs with write intent log support	Maximum LUNs per consistency group	Maximum consistency groups per array
AX4-5	25	8	8
CX3-10c	25	8	8
CX3-20	50	8	8
CX3-40	100	16	16
CX3-80	100	16	16
CX4-120	128	16	64
CX4-240	256	16	64
CX4-480	512	32	64
CX4-960	512	32	64

Table 3. Mirroring limits on CLARiiON storage systems with MirrorView/A

CLARiiON model	Max mirrored pairs	Maximum LUNs per consistency group	Maximum consistency groups per array
AX4-5	25	8	8
CX3-10c	25	8	8
CX3-20	50	8	8
CX3-40	100	16	16
CX3-80	100	16	16
CX4-120	100	8	50
CX4-240	100	8	50
CX4-480	100	16	50
CX4-960	100	16	50

Planning to virtualize Exchange

If you are considering using SRM to protect your Exchange environment, it means that either you are already running Exchange on VMware virtual machines, or are planning to migrate to that platform. On the VMware website there is a collection of information on running Exchange. The EMC white paper *Transitioning Exchange 2003 to VMware Virtual Exchange 2007 Using EMC CLARiiON – Best Practices Planning*, which can be found on EMC.com and the VMware website, is also helpful.

Additional considerations:

- The Exchange servers at both sites should be within the same Windows domain.
- There should be two Active Directory servers (domain controller/global catalog server) at each site.
- Windows 2008 x64 is required for SVVP compliance.
- SRM cannot be configured as an application for failover with Microsoft Windows clusters. If your current Exchange server is on a clustered machine (shared quorum or majority node set), we recommend using mailbox migration to move the mailboxes to the new non-clustered virtualized Exchange server. SRM will provide for rapid disaster recovery protection at the second site. Cluster-equivalent local protection for a failed server is provided by VMware HA, which can seamlessly shift an Exchange VM to an alternate associated ESX server.
- The Exchange server at the recovery site can be on a different subnet. In this case you need to create a customized specification within VMware providing the IP address of the Exchange server after failover.
- Exchange 2007 is supported.

Setup

The setup for SRM protection of Exchange is very similar to the standard SRM configuration. The amount of extra work depends mostly on the starting Exchange environment. If your Exchange mailbox server is not already running within a VMware virtual machine, start by configuring a new mailbox server on a VM and then using standard Exchange mailbox migration between your existing physical Exchange server and the new virtual Exchange server.

Once the Exchange server is operating within the virtual machine and you have configured the Exchange database and log LUNs, use Navisphere® to configure the mirrors of these LUNs to the associated CLARiiON storage system at the DR site.

Take the following into consideration when you build your virtualized Exchange server and configure mirroring for its LUNs:

- The number of Exchange users that a virtualized server can support is typically similar to the number of users that can be supported on the physical machine. The memory and CPU resources allocated for the Exchange VM should meet the standard Microsoft guidelines for Exchange servers. In addition, there should be some extra CPU and memory resources reserved on the VMware server for ESX itself.

  There is currently a recommended limit of 4,000 Exchange users within a VM. This does not necessarily decrease the number of users that a physical ESX server can support, but it may require distributing the users among more VMs.
- Standard Exchange best practice recommendations apply for the virtualized Exchange server configuration. These include:
  - Use a single database file for each Exchange storage group.
  - Keep the database LUN and log LUN for the same storage group on separate spindles.
  - Apply EMC Exchange building block configurations for validated performance levels.
- Typically all Exchange LUNs on one server plus the guest operating system (GOS) for that server will be in one SRM protection group. SRM works with MirrorView consistency groups, and often you can combine the LUNs on one Exchange server (data LUNs plus GOS) all within the same consistency group. As mentioned above, there may be situations when you must use multiple consistency groups to stay within CLARiiON limits.
- When creating mirrors, use the write intent log, which will provide added protection in the unlikely event of the loss of a storage processor.
- SRM protection of the Exchange Client Access Server (CAS) is not necessary. There should be a CAS server configured at each site within the same Windows domain.
- Incoming messages go to the Hub Transport server before reaching the Mailbox server. You can protect these additional in-flight messages by replicating the Hub Transport server with SRM.

Normal operation

In normal day-to-day operation of the Exchange environment, SRM provides transparent protection without any need for administrative action. However, SRM includes a convenient nondisruptive way to confirm failover readiness, and it is advisable to perform this check on a regular basis. This section describes the SRM failover test process for Exchange, and also some other normal administrative operations.

Testing failover

SRM recovery plans include a valuable testing feature that allows an administrator to test a near-complete failover of Exchange production to the DR site – without the need to bring down users. When you manually perform a failover test of an SRM protection group, SRM will administer the following actions:

- Leave the production VM running, so that existing Exchange users remain online and functional.
- Disable the pertinent network connections at the recovery site to avoid a conflict with the same Exchange server being mounted at both sites.
- Start a snap session at the recovery site for each mirrored target LUN in the protection group being tested.
- Mount the snapshots (read/write) to the server at the recovery site.
- Start the Exchange VM at the recovery site (with the network disabled).
- Clean up test resources after the test is complete.

The test is considered successful if the VM starts at the recovery site. You can further check it by logging onto the VM console. You can run an eseutil check on the mounted snap, but this should be run during a period of low user activity to avoid affecting the mirroring performance. You can even have a test domain/network at the remote site configured through VMware so you can test the Exchange environment with users connected.

MirrorView/S is and MirrorView/A may be mirroring production data during and after this test. When snap sessions are active, there is some additional overhead that can increase the mirroring response times. For this reason, EMC recommends that you run these failover tests during off-hours. After verifying the test has been successful, it is important to remember to return to the VMware Virtual Infrastructure console and click the **Continue** button within the SRM plug-in. This cleans up the storage after the test, including removing the snap sessions.

Although it involves a short amount of downtime for users, for a complete guarantee that you are prepared to perform a successful failover, you should perform a true failover of the production environment to the recovery site as part of the initial configuration, and on a regular basis thereafter. To ensure site DR preparedness, it is recommended that a regularly scheduled failover between sites be done. This will increase the familiarity of the failover and disaster processes required, thus guaranteeing a smooth transition if a true disaster occurs.

Handling reconfiguration

Adding/removing an Exchange storage group

To add a new Exchange storage group to an existing SRM protection group, the steps are:

1. Create the new Exchange LUNs.

2. Add the new LUNs to an existing consistency group (all mirrors within a CG are synchronized at the same time).

   This will cause the added LUNs to show up within the SRM console. A rescan may be necessary. From this point on the new LUNs will be considered as part of that SRM protection group.

If you remove an Exchange storage group and its associated LUNs from the consistency group, they will automatically be removed from the SRM protection group.

Adding/removing an Exchange VM

To add or remove an Exchange mailbox server VM, follow the basic instructions for adding/removing an SRM protection group.

Optimizing performance

When protecting the Exchange environment with synchronous mirroring, even with the additional mirroring overhead it is important that the key Exchange response times stay within the published Microsoft guidelines for efficient production operation.

To operate within these limits, apply Exchange storage best practices to achieve the best possible local response time (before adding mirroring). Then take whatever steps possible to minimize the additional latency caused by the mirror. This includes choosing a close site for DR (when possible – a second site 10 miles away will generally cost less latency than a site 50 miles away). It also means applying networking best practices to minimize delays in the path between the sites.

If the CLARiiON array is being used for other applications besides Exchange, the Navisphere Quality-of-Service Manager (NQM) can be used to give various levels of priority to the mirrored LUNs so that their key latency parameters can be maintained.

Be aware that a true SRM failover to the recovery site requires a complete resynchronization of all mirrored LUNs in the protection group (unless the mirrored links remain consistent). For this reason, whenever possible, take advantage of the SRM test failover capability rather than perform a true production failover. If you do need to resynchronize the mirrors, be aware that all mirrors within a consistency group must be synchronized at the same time. When possible it is best to perform this synchronization during off-hours to complete it in the shortest possible time.

While this is not SRM-specific, there are certain scenarios in which the performance of a set of Exchange LUNs within a RAID group has degraded (such as the user's IOPS requirements increasing over time due to added mobile usage, and so forth). In this case, you can resolve the issue in a variety of ways. Some users could be migrated out of the storage group. CLARiiON includes a LUN migration feature that would allow a transparent move of the impacted Exchange LUNs to faster drives, or to a faster RAID configuration (such as RAID 5 to RAID 10). This can remove the performance bottleneck without requiring users to be moved.

Failover

Failover with SRM and MirrorView is a straightforward, manually initiated process. Because you have set up a recovery plan as part of the SRM configuration, there are very few steps needed to move your production virtual machine from the protected site to the recovery site. In most cases the process is not any different with an Exchange virtual machine.

MirrorView/S synchronously keeps the Exchange mirrored targets up to date at the recovery site, so the recovery point objective (RPO) will be zero. With MirrorView/A the RPO depends on the frequency of the updates. In either case the recovery time objective (RTO) can be as low as a few minutes to switch over a single VM.

The standard failover steps are:

1. Administrator determines that a failover is required.

2. The administrator logs in to the VMware Virtual Infrastructure client at the recovery site and initiates the SRM recovery plan for the appropriate protection groups.

3. SRM promotes the mirrored target LUNs to the ESX server at the recovery site.

4. The virtual machine is started up on the ESX server at the recovery site.

5. Exchange services start up automatically as part of the startup of the VM.

If the VMs at the recovery site are on a different subnet from the VMs at the protected site, you must go through a few additional steps before the new Exchange VM can be accessed by users. These steps can be automated. If you created a customized specification make sure the recovery plan for the VM being protected has the associated customization specification file associated with it. If not, you can manually change the parameters by logging in to the Exchange server and changing the IP address.

Failover is fast and easy. Failback involves more steps and time, but unlike an unplanned failover you can schedule a failback for when it is more convenient. Use the failover test feature in SRM for periodic tests of the process. Test failovers do not require any failback steps. For best protection against individual server failures, you can use VMware HA, which transparently shifts the affected VMs on a failed ESX server over to another functioning server at the same site, attached to the same storage.

Additional failure scenarios

SRM is intended primarily to protect against the loss of an entire site, including servers and storage. Because failover is manual, there are a few other scenarios where an administrator needs to consider initiating the SRM recovery plan, or otherwise adjusting the mirroring configuration.

Loss of the mirrored link

With MirrorView/S, if the mirroring link between the two arrays goes down for more than a few minutes the mirrors are automatically fractured, and MirrorView maintains a copy of the writes to the primary image until the link has been re-established. With MirrorView/A, the changes will continue to be tracked and are used to update the secondary image when the link comes back.

If the link is down for an extended period, it can reach the point where it is best to perform a complete resynchronization after the link is restored. Before the start of a resynchronization, the mirrored target LUNs at the recovery site are all valid and consistent, but they are up to date only to the point where the link failed. In the event of a link failure followed by a primary site failure you can initiate the SRM recovery plan but there will be data loss equivalent to the amount of time that the link has been down (for example, the un-mirrored data), so the failover must considered carefully.

Typically the mirrored target LUNs at the recovery site represent the most current replica of Exchange data. For that reason, it is important to preserve this data prior to beginning a full synchronization from the protected site. The synchronization will overwrite the mirrored replica and will be unusable until the sync completes. For normal updates MirrorView/A protects the secondary image with a snapshot until the update finishes. Upon successful completion of the update, the snapshot is destroyed.

To confirm that you always have a recoverable copy of Exchange data at the recovery site with MirrorView/S:

- Set the recovery policy for the mirrors to **Manual**, so that synchronization does not start until you are ready for it.
- Take a copy of the mirrored target LUNs before they are overwritten by the synchronization process. The safest and most flexible way to do this is to create clones of these LUNs (EMC Replication Manager can help automate this). You can take snapshots, but this may slow down the speed of the synchronizations. You can also back up the LUNs to disk or tape.

SP failure

In the unlikely event of the failure of one of the two storage processors (SPs) on a production CLARiiON array, all LUNs associated with the failed SP trespass to the functioning SP. SRM itself is not affected by the loss of an SP. On CLARiiON CX3 models and earlier models, write caching is turned off when an SP fails.

On the new CX4 models, there is more write cache available and this cache remains active during an SP failure. While it is still especially important to monitor Exchange performance when one of the SPs is down, the CX4 is more likely to be able to handle a continuation of production, including mirroring.

Failback

As mentioned previously, failing back to the original production site is more involved than the process of failing to the recovery site. The standard process for failing back to the original protected site with SRM involves these general steps:

1. Rebuild to the original production environment as necessary, including:

    a. Restoring the array, servers, and other infrastructure.

b. Updating the MirrorView configuration and establishing the network links.

c. Cleaning up the mirrors and consistency groups at the recovery site in preparation for failback.

2. Clearing out the previous SRM recovery plan and creating a new plan for failing back the protection groups.

3. Updating the SRM recovery plan.

4. Reconfiguring the new mirrors and consistency groups.

5. Performing a full synchronization of the LUNs back to the original production site.

6. Initiating the SRM recovery plan to move the VMs back to the original site

This process is detailed more completely in the *VMware Site Recovery Manager Administration Guide*, and also in the *VMware Site Recovery Manager with EMC CLARiiON CX3 and MirrorView/S Implementation Guide*.

As with failover, there is minimal additional work when the VMs are Exchange servers. If Exchange services are installed and configured to start automatically when the server starts, then the failed-back Exchange VM becomes available to users as soon as SRM completes the recovery plan and makes the VM available at the recovery site.

As soon as possible after the original site is back in production, you should reconfigure the mirrors and SRM recovery plans to restore DR protection. This involves a straightforward re-creation of the SRM recovery plans, and a reversal in the direction of the mirrors (this does not require any resynchronization).

Conclusion

VMware Site Recovery Manager combined with EMC MirrorView provides an excellent disaster recovery solution for virtualized Exchange mailbox servers. It offers pre-determined recovery plans that re-establish the Exchange production environment very quickly at the recovery site. With synchronous MirrorView, it can do this with zero data loss, while asynchronous MirrorView provides a relatively low RPO and can replicate far distances.

Most IT organizations today have either committed to moving to a mostly virtualized environment or they are seriously considering this option, because of its compelling cost-savings potential. There have been reasons, relating to performance and support, to be more cautious with virtualizing Microsoft Exchange than with most other applications. However, as more organizations find they can run virtualized Exchange successfully, and as Microsoft becomes more accepting of virtualized Exchange, there has been a ramp-up in implementations. SRM with MirrorView is a valuable new solution for this new way of running Exchange, taking best advantage of the cost savings and high-level protection made possible with VMware and CLARiiON shared storage.