



EMC MirrorView Adapter for VMware Site Recovery Manager

Version 1.4

Release Notes
P/N 300-007-019
REV A06
October 5, 2009

These release notes contain supplemental information about the EMC[®] MirrorView[®] Adapter for VMware Site Recovery Manager (SRM).

Topics include:

- ◆ Revision history..... 2
- ◆ Product description 2
- ◆ New features and changes..... 2
- ◆ Fixed problems 3
- ◆ Environment and system requirements..... 3
- ◆ Known problems and limitations 5
- ◆ Technical notes 7
- ◆ Documentation 16
- ◆ Software media, organization, and files 16
- ◆ Installation 17
- ◆ Troubleshooting and getting help 21

Revision history

Revision	Date	Description
A06	Oct 05,2009	Adds support for SRM 4.0 , FLARE 04.29 and includes MirrorView Insight for VMware(MVIV)
A05	Jan 08,2009	Adds support for individual mirrors as well as consistency groups
A04	Sep 30, 2008	Adds AX4-5 and MirrorView/A Support
A03	Aug 4, 2008	Adds CX4 support
A02	June 12, 2008	Adds information on the VMware support page on Powerlink
A01	May 12, 2008	First release of product

Product description

The MirrorView® Adapter is a software package that allows the VMware Site Recovery Manager (SRM) to implement disaster recovery for ESX Server 3.X virtual machines using CLARiiON® CX3 series, CX4 series, and AX4-5 dual-SP storage systems running MirrorView/S or MirrorView/A and SnapView® replication software. This adapter supports MirrorView/Synchronous (MirrorView/S) or MirrorView/Asynchronous (MirrorView/A) over both iSCSI and Fibre Channel direct and SAN connections.

MirrorView/S is synchronous MirrorView and MirrorView/A is asynchronous MirrorView.

For more Site Recovery Manager configuration details and best practices, select **VMware Support** on the **Navigator** drop-down menu at the top right of the EMC Powerlink® (<http://Powerlink.EMC.com>) home page (registration required).

New features and changes

- ◆ Support for SRM 4.0 and FLARE 04.29
- ◆ Includes MirrorView Insight for VMware(MVIV)



If you are upgrading from the previous version of the adapter (1.0 or 1.1), see “Upgrading the MirrorView Adapter” in the Technical Notes section.

Fixed problems

Visit the EMC Powerlink® Issue Tracker website at <http://Powerlink.EMC.com> for the most recent updates to this MirrorView Adapter version.

Platforms	Brief description	Symptom details	Solution (or workaround)
All supported platforms	<p>Solutions Enabler Recovery plan test run fails. 195191 <u>Frequency of occurrence:</u> Always <u>Severity:</u> High</p>	When snapshot names and consistency group names contain <i>any non-alpha numeric characters</i> , Solutions Enabler API fails.	<p>Fixed in code. <u>Exists in version:</u> Solutions Enabler 6.5.0 <u>Fixed in version:</u> Solutions Enabler 6.5.1</p>
All supported platforms	<p>Solutions Enabler Failover test fails. 195619 <u>Frequency of occurrence:</u> Limited <u>Severity:</u> High</p>	<p>During the failover test, the following error message may appear in the logs: The operation cannot be completed because the LUN specified is in use by an array feature. The error may be caused by the lack of reserved LUN pool resources for the snapshots. Each source LUN requires at least one reserved LUN.</p>	<p>Fixed in code. In this scenario the following error message will be logged: The operation cannot be completed because there are no available, unallocated SnapView save area LUNs Verify that you have configured SnapView as described in the SnapView configuration guidelines in the Navisphere Manager help. <u>Exists in version:</u> Solutions Enabler 6.5.0 <u>Fixed in version:</u> Solutions Enabler 6.5.1</p>

Environment and system requirements

The VMware infrastructure at *both* the protected (primary) and recovery (secondary) sites must meet the following requirements:

- ◆ VirtualCenter Server version 2.5 update 4 or vSphere 4.0
- ◆ VI Client 2.5 or vSphere Client 4.0
- ◆ Site Recovery Manager (SRM) Server with the following installed:

SRM version 1.0 or SRM 1.0 Update1 or SRM 4.0
 EMC Solutions Enabler version 7.0.1 or later.
 EMC MirrorView Adapter version 1.4

This server can be the VirtualCenter server or a separate host running one of the following windows operating systems:

Windows Server 2003 SP1 (x86, x64)
 Windows Server 2003 R2 (x86, x64)
 Windows Server 2008 (x86, x64)

Operating system support for SRM Sever varies depending on the SRM version. Please refer to SRM documentation for the supported versions.

- ◆ One or more ESX servers connected to CLARiiON storage systems. ESX Sever compatibility varies with SRM version. Please refer to SRM documentation for supported versions and patch levels.

MirrorView Adapter compatibility matrix

Storage replication adapter compatibility list for EMC MirrorView Adapter v1.4	CLARiiON Software Name and Version		
	CLARiiON Hardware Models	FLARE® Operating Environment	Navisphere Manager
CX3-10c, CX3-20c, CX3-20f, CX3-40c, CX3-40f, CX3-80	03.26	06.26	MirrorView/S 03.26 MirrorView/A 03.26 SnapView 03.26 Solutions Enabler 7.0.1
CX4-120, CX4-240, CX4-480, CX4-960	04.28	06.28	MirrorView/S 04.28 MirrorView/A 04.28 SnapView 04.28 Solutions Enabler 7.0.1
	04.29	06.29	MirrorView/S 04.29 MirrorView/A 04.29 SnapView 04.29 Solutions Enabler 7.0.1
AX4-5 with the Navisphere Manager enabler and expansion pack enabler installed	02.23	06.28	MirrorView/S 02.23 MirrorView/A 02.23 SnapView 02.23 Solutions Enabler 7.0.1

Celerra Hardware Models	FLARE® Operating Environment	Navisphere Manager	Replication software
NS120F (Backend CX4-120) NS480F (Backend CX4-480) NS960F (Backend CX4-960)	04.28	06.28	MirrorView/S 04.28 MirrorView/A 04.28 SnapView 04.28 Solutions Enabler 7.0.1
NX4F (Backend AX4-5)	02.23	06.28	MirrorView/S 02.23 MirrorView/A 02.23 SnapView 02.23 Solutions Enabler 7.0.1

CLARiiON storage-system requirements

The CLARiiON storage system at each site must:

- Have the SnapView, MirrorView /S and/or MirrorView / A enablers installed.
- Be connected and configured as described in “Connecting the storage systems” and “Configuring the storage for Site Recovery Manager” in the Technical notes section.

The storage system at the protected site is the primary storage system and the storage system at the recovery site is the secondary storage system.

Known problems and limitations

Known problems

Visit the EMC Powerlink Issue Tracker website at <http://Powerlink.EMC.com> for the most recent updates.

Platforms	Symptom details	Problem description	Prevention/resolution or workaround
All supported platforms	VMware SRM SRM service fails to start. <u>Frequency of occurrence:</u> Always <u>Severity:</u> Medium <u>VMware PR#</u> 330567	If the array manager (SRA) is uninstalled or if the SRA manifest file was changed, missing, deleted or corrupted, SRM service fails to start.	Reinstall the adapter and restart the SRM service <u>Exists in version:</u> VMware SRM 1.0, 1.0 U1, 4.0

Known problems and limitations

Platforms	Symptom details	Problem description	Prevention/resolution or workaround
All supported platforms	<p>VMware SRM</p> <p>More than one peer storage system is not supported by SRM.</p> <p><u>Frequency of occurrence:</u> Always</p> <p><u>Severity:</u> Medium</p> <p><u>VMware PR#</u> 330567</p>	<p>VMware SRM does not support a “one to many” configuration. In a scenario where a CLARiiON is replicating to multiple CLARiiON storage systems, during storage-system discovery you will encounter the following error message:</p> <pre>LUNs with different peer array keys received from SAN integration scripts</pre>	<p>See the “Working with more than one peer storage system” topic in the Technical Notes section.</p> <p><u>Exists in version:</u> VMware SRM 1.0, 1.0 U1, 4.0</p>
All supported platforms	<p>VMware SRM</p> <p>While running planned failover scenarios, MirrorView mirrors may go “out-of-sync (waiting-on-admin state)” after failover.</p> <p><u>Frequency of occurrence:</u> Sometimes</p> <p><u>Severity:</u> Limited</p>	<p>While executing the planned failover (recovery plan) the I/O to the MirrorView source images is not quiesced by SRM or ESX servers resulting in “out-of-sync (waiting-on-admin state)” mirrors after failover.</p>	<p><u>Exists in version:</u> VMware SRM 1.0, 1.0 U1, 4.0 VMware ESX Server 3.0.2, 3.5, 4.0</p>
All supported platforms	<p>EMC MirrorView SRA</p> <p>While running simultaneous recovery plans, only the first recovery plan succeeds.</p> <p><u>Frequency of occurrence:</u> Always</p> <p><u>Severity:</u> Limited</p>	<p>EMC MirrorView Adapter blocks running (simultaneously) more than one recovery plan to prevent returning inconsistent information to SRM.</p>	<p>Run the recovery plans sequentially.</p> <p><u>Exists in version:</u> EMC MirrorView SRA 1.0, 1.1, 1.2, 1.3, 1.4</p>

Limitations

- ◆ Before configuring the Site Recovery Manager at each site, you must configure the appropriate storage in the CLARiiON storage system at each site, as described in “Configuring the storage for Site Recovery Manager” in the next section.
- ◆ Configuration validation is limited.

- ◆ Site Recovery Manager does not perform an automatic failback after a failover occurs. When a failover occurs, re-establish the MirrorView configuration and perform a manual failback as described in the technical notes section “Restoring a failed site.”
- ◆ Unlike MirrorView/S, MirrorView/A uses scheduled or manual updates to replicate the changes between primary and secondary images. Recovery operation (Consistency Group or Mirror Promote) is not allowed while a group or mirror update is in progress.
You can insert a message step in the recovery plan (before “Prepare Storage”) to check the mirror state or to manually synchronize the mirrors using Navisphere. You must wait until the mirror synchronization completes before resuming the execution of the recovery plan.

Technical notes

This section describes:

- ◆ MirrorView consistency groups and SRM protection groups
- ◆ Connecting the storage systems
- ◆ Configuring the storage for Site Recovery Manager
- ◆ Working with more than one peer storage system
- ◆ Determining the version of the MirrorView Adapter that is installed on an SRM server
- ◆ MirrorView/A
- ◆ Restoring a failed site
- ◆ MirrorView Insight for VMware (MVIV)

MirrorView consistency groups and SRM protection groups

MirrorView supports consistency groups. A consistency group is a set of synchronous or asynchronous mirrors whose secondary images must be kept consistent with each other to be recoverable or crash-consistent. This consistency allows an application to use the secondary images if the primary storage system fails.

An SRM protection group is a set of virtual machines (VMs) that are failed over together during test and recovery.

When establishing the relationship between a MirrorView consistency group and an SRM protection group, you must follow these guidelines:

- ◆ A VM is backed by multiple LUNs if the VM meets any of the following conditions:
 - The VM is located on a datastore having extents on multiple LUNs.
 - The VM is either located on or using multiple datastores (for example, the extra hard disk for the VM comes from another datastore).
 - The VM has RDM or RDMP LUNs. (Refer to SRM administrators guide for supported configurations with RDM and RDMP LUNs.)
- ◆ All the source LUNs and their mirrors for the VMs in a protection group should be part of the same consistency group, unless the limit for LUNs in a consistency group is exceeded, in which case they can be in multiple consistency groups.
- ◆ Since all the LUNs (mirrors) in a consistency group are failed over together, these consistency groups must *not* contain any other LUNs (mirrors).

Connecting the storage systems

You must set up the storage-system hardware as follows:

- ◆ Mirror ports on SP A in the primary (source) and secondary (target) storage systems must be connected, and the mirror ports on SP B in the primary and secondary storage systems must be connected. For information about determining which port is your MirrorView port see the Navisphere Manager online help.

You can use the mirror ports for host data, but you should be cautious about sharing ports between MirrorView and host traffic when an IP distance connection is used because sharing ports between MirrorView and host traffic may cause a degradation in both replication and server application performance.

- ◆ At each site, the storage-system management ports must be on the *same* network as the Site Recovery Manager server and the VirtualCenter at the site.
- ◆ The protected ESX Server hosts must be connected to the primary storage-system data ports and the recovery ESX Server hosts must be connected to the secondary storage-system data ports.
- ◆ At the recovery site, the ESX Server hosts for the recovery virtual machines must be connected to the secondary storage-system data ports.

Configuring the storage for Site Recovery Manager

During failover testing, the MirrorView Adapter uses SnapView snapshots. When you create a SnapView snapshot of a LUN for a virtual machine, the name of the snapshot must include the following text string: **VMWARE_SRM_SNAP**. During failover testing, the MirrorView Adapter looks for this text string in the name of the inactive snapshot(s) for the virtual machine LUN(s) and creates a consistent snap session for this snapshot(s). When failover testing is finished, the MirrorView Adapter stops the SnapView session automatically.

Use Navisphere Manager or Navisphere Secure CLI to configure the primary storage system for each protected ESX Server host connected to the primary storage system and to configure the secondary storage system for each recovery ESX Server host connected to the secondary storage system. For each supported hardware platform the number of LUNs you can mirror, the number of consistency groups you can create, and the number of mirrors each consistency group can contain varies. Please refer to the MirrorView documentation available on the Powerlink website: <http://Powerlink.EMC.com>.

To configure storage on the storage systems:

Refer to Figure 1 for a sample configuration.

1. On the primary storage system, create a storage group and assign it to the protected ESX Server host connected to it.
2. On the secondary storage system, create a storage group and assign it to the recovery ESX Server host connected to it.
3. For *each* LUN required for a virtual machine that the SRM will protect:
 - a. On the primary storage system, create a source LUN and assign it to the storage group for the protected ESX Server host.
 - b. Create a SnapView snapshot of the source LUN and assign it to the storage group for the protected ESX Server host.

The MirrorView Adapter activates and uses this snapshot during data recovery failback, when the original primary image is temporarily demoted to the secondary image.

- c. On the secondary storage system, create a matching destination LUN.

- d. Create a SnapView snapshot of the destination LUN and assign it to the storage group for the recovery ESX Server host.

The MirrorView Adapter activates and uses this snapshot of the secondary image during data recovery testing.

- e. On the primary storage system, create a mirror containing the primary LUN and the secondary LUN that you just created.
 - f. Assign the secondary LUN to the storage group for the recovery ESX Server host.
4. Create a consistency group (on the primary storage system) that contains all the mirrors for the virtual machine.

A corresponding consistency group is created automatically on the secondary storage system.

A consistency group is not required, but recommended as long as the number of consistency groups limit is not reached for your CLARiiON hardware model.

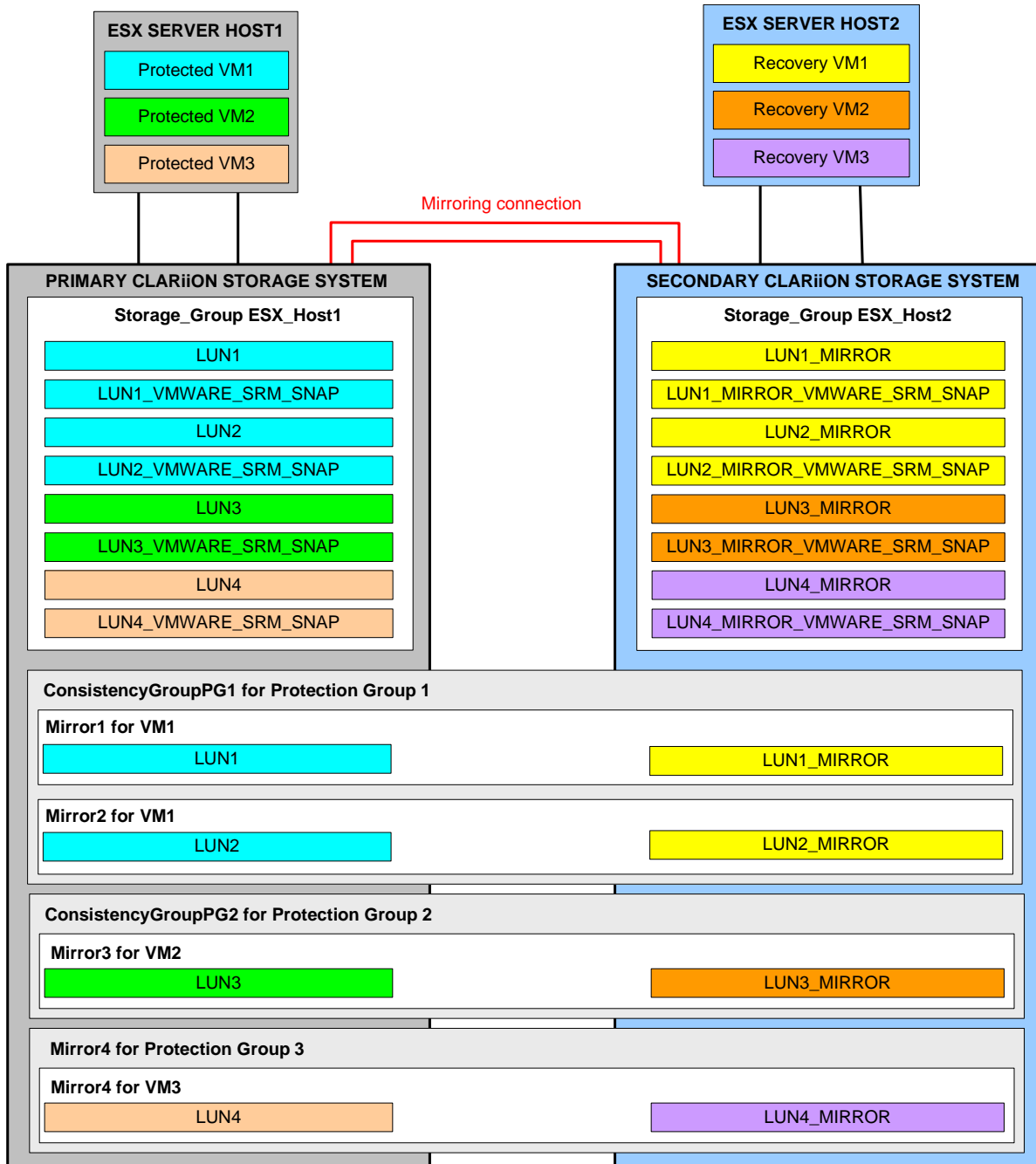


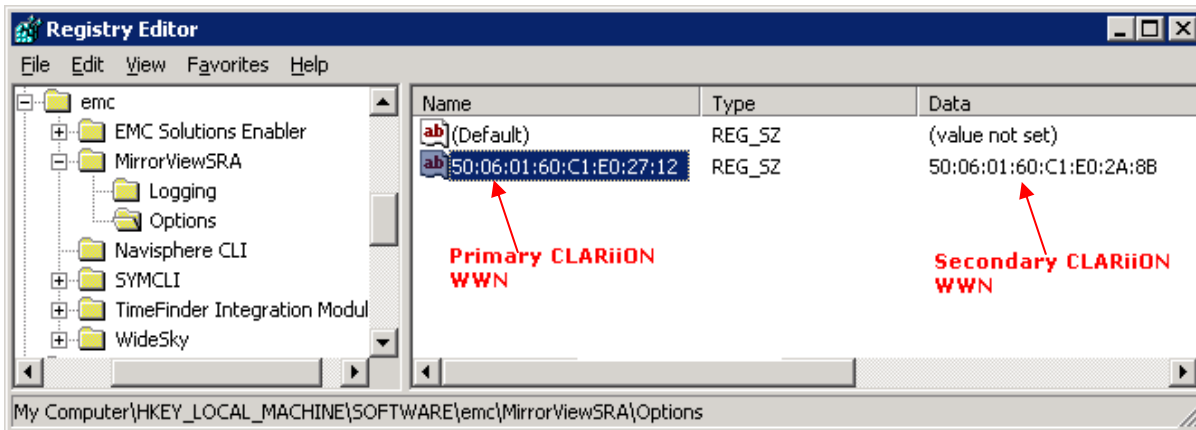
Figure 1 Sample primary and secondary storage-system configuration

Working with more than one peer storage system

MirrorView supports multiple peer storage systems (arrays); in other words, one CLARiiON storage system can be replicating to multiple secondary CLARiiON storage systems. EMC MirrorView Adapter supports this configuration. However SRM 1.0 does not support a “one to many” configuration. In a scenario where a CLARiiON storage system is replicating to multiple CLARiiON storage systems, during storage system discovery you will encounter the following error message:

LUNs with different peer array keys received from SAN integration scripts

As a work around in this scenario, you have to choose which secondary CLARiiON storage system should be reported by the adapter to SRM. On both SRM servers, you can specify the primary to secondary mapping in the registry under “HKEY_LOCAL_MACHINE\SOFTWARE\emc\MirrorViewSRA\Options”.



When this mapping is present in the registry, EMC MirrorView adapter will report only the consistency groups or mirrors that are replicating between these storage systems.

Determining the version of the installed MirrorView Adapter

Run the following command from the command prompt to determine the version of the MirrorView Adapter that is installed on an SRM server:

MirrorViewSRACLI.exe -v

MirrorViewSRACLI.exe is in the installation directory of the MirrorView Adapter. The default location of the installation directory is **C:\Program Files\VMware\VMware Site Recovery Manager\scripts\SAN\MirrorView SRA**

MirrorView/A

Unlike MirrorView/S, MirrorView/A uses scheduled or manual updates to replicate the changes between primary and secondary images.

A recovery operation (Consistency Group or Mirror Promote) is not allowed while a mirror update is in progress. You can insert a message step in the recovery plan (before "Prepare Storage") to check the mirror state or to manually synchronize the mirrors using Navisphere. You must wait until the mirror synchronization completes before resuming the execution of the recovery plan.

Restoring a failed site

If a site fails and the MirrorView connection between the primary and secondary storage system is down, then a local only promote may occur on the remote site.

Failback when a local only promote does *not* occur

If the local only promote does *not* occur and the mirror state after promote is "consistent" or "synchronized", you do *not* need to do anything on the CLARiiON storage system. Follow the failback procedure in the *VMware Site Recovery Manager Administration Guide*.

If the mirrors are "out-of-sync" or "waiting-on-admin" state you need to synchronize the mirrors before attempting a failback.

Failback when a local only promote does occur

1. Power up the storage system at the failed site.
2. Restore MirrorView and the IP links.

3. For each consistency group that is locally promoted, use Navisphere Manager to do the following:
 - a. Destroy the consistency group on both CLARiiON storage systems.

To destroy a consistency group that contains mirrors, open the properties dialog box for the consistency group, and click **Force destroy**.
 - b. Destroy the remote mirrors on the CLARiiON storage system at the failed site.

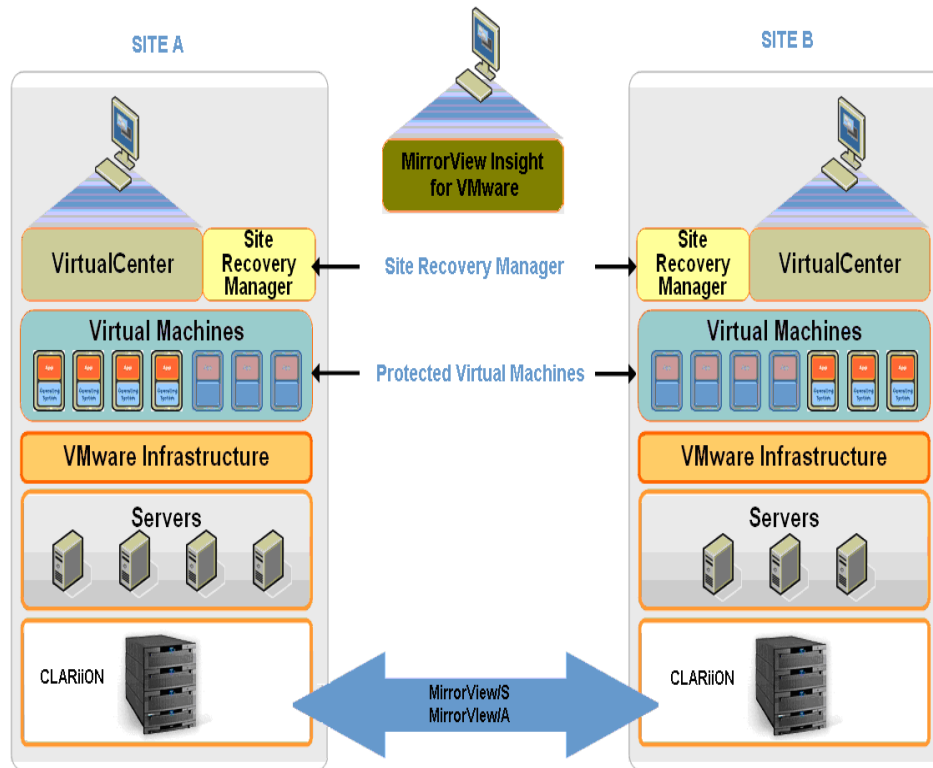
To destroy a mirror, open the properties dialog box for the mirror, select the Primary image tab, and click **Force destroy**.
 - c. Remove the LUNs, which were in the mirrors you destroyed, from the storage group on the CLARiiON storage system at the failed site.
 - d. Right-click each remote mirror on the CLARiiON storage system at the surviving site, select **Add Secondary Storage**, and choose the LUN from the CLARiiON at the failed site.
 - e. Create a new consistency group with the same name as the one you destroyed, and add the remote mirrors that were part of the destroyed consistency group to this new consistency group.
 - f. Add the LUNs that you removed from that storage group at the failed site back into the storage group on the CLARiiON storage system at the remote site.
4. For each mirror (not in a consistency group) that is locally promoted, use Navisphere Manager to do the following:
 - a. Destroy the remote mirrors on the CLARiiON storage system at the failed site.

To destroy a mirror, open the properties dialog box for the mirror, select the Primary image tab, and click **Force destroy**.
 - b. Remove the LUNs, which were in the mirrors you destroyed, from the storage group on the CLARiiON storage system at the failed site.
 - c. Right-click each remote mirror on the CLARiiON storage system at the surviving site, select **Add Secondary Storage**, and choose the LUN from the CLARiiON at the failed site.
 - d. Add the LUNs that you removed from that storage group at the failed site back into the storage group on the CLARiiON storage system at the remote site.

5. Follow the failback procedure in the VMware Site Recovery Manager Administration Guide.

MirrorView Insight for VMware (MVIV)

MVIV is bundled along with the adapter and provides insight into MirrorView replication environment with respect to VMware infrastructure.



MVIV supports the following ESX and Virtual Center versions:

ESX Server 3.5 Update 4 , ESX Server 4.0

VirtualCenter 2.5 Update 4, vSphere 4.0

An SRM administrator can use MVIV to view the replication configuration of their virtual infrastructure. MVIV also offers an experimental failover and failback capability to troubleshoot the SRM configuration before using the configuration for production.

Documentation

The following lists the documentation applicable to this product version:

Part number	Description
None	VMware Site Recovery Manager Administration Guide available from VMware website: http://www.vmware.com/ .
None	Navisphere Manager help available from the Navisphere Manager user interface and the Navisphere Management Suite section of Technical Documentation and Advisories on the Powerlink website: http://www.Powerlink.EMC.com .
069001184	EMC MirrorView/Synchronous Command Line Interface (CLI) Reference
300-001-335	EMC MirrorView/Asynchronous Command Line Interface (CLI) Reference

For more Site Recovery Manager configuration details and best practices, select **VMware Support** on the **Navigator** drop-down menu at the top right of the EMC Powerlink® (<http://Powerlink.EMC.com>) home page (registration required).

Software media, organization, and files

The following table lists the file for this version of the MirrorView Adapter plug-in:

Filename	Description
EMC_MirrorView_Site_Recovery_Adapter-1.x.y.z.exe where x.y.z specifies the version number.	EMC MirrorView Adapter plug-in installer available from the VMware website: http://www.vmware.com/download/srm/ .

Installation

You must connect and configure the CLARiiON storage systems for each protected virtual machine before you configure the Site Recovery Manager. The “Connecting the storage systems” and “Configuring the storage for Site Recovery Manager” sections have information on storage-system hardware setup and storage configuration.

Before installing the MirrorView Adapter (MirrorView SRA), the following must be done:

1. Install the VMware Site Recovery Manager on a supported Windows host (the SRM server) at both the protected and recovery sites.
2. Install EMC Solutions Enabler on both the protected and recovery SRM servers.

You can download the EMC Solutions Enabler from the Downloads and Licensing section on the Powerlink website (<http://Powerlink.EMC.com>).

Upgrading the MirrorView Adapter



If you are upgrading from the previous version of the adapter (1.0 or 1.1), follow the instructions below. If you are upgrading from adapter version 1.2, you can ignore this section.

With this version, adapter name changed from MirrorView SRA to EMC MirrorView SRA.

If you configured the SRM using the previous version of the adapter (that is, you configured the array managers, protection groups and recovery plans), upgrading to this version of adapter will prevent SRM service from restarting. This is a symptom of VMware problem report # 330567, details of which are as follows:

VMware PR# 330567: In SRM version 1.0, if the array manager (SRA) is uninstalled or if the SRA manifest file changed, missing, deleted or corrupted ... SRM service fails to start and you will see the following error message in the SRM logs.

```
[2008-09-14 22:34:59.234 'PrimarySanProvider' 312 verbose] Loading Array Manager 'array-manager-14875' from DB object
```

```
[2008-09-14 22:34:59.250 'DrServiceInstance' 312 warning] Initializing service content: Unexpected MethodFault (dr.san.fault.ManagementSystemNotFound) {
```

```
  dynamicType = <unset>,
  name = "MirrorView SRA",
  msg = ""
}
```

To avoid this issue, follow the steps below before upgrading the array manager. These steps are required unless you are working with a version of SRM that includes fix for PR#330567.

1. Take an inventory of your protection groups and recovery plans because you have to recreate them after upgrading the adapter.
2. On the recovery site SRM Server, remove all the recovery plans related to MirrorView SRA.

If you have any recovery plans configured on the protected site SRM Server (this is not typical, but possible in a configuration where each site is configured to act as a recovery site as well as protected site), remove them also.

3. On the protected site SRM Server, remove all the protection groups related to MirrorView SRA.

If you have any protection groups configured on the recovery site SRM Server, remove them also.

4. On the protection side SRM server:
 - a. Click array managers **configure**.
 - b. Click **Next** to move to Recovery Side Array Managers.
 - c. Remove all MirrorView SRA Recovery Side Array Managers.
 - d. Click **Back** to move to Protection Side Array Managers.
 - e. Remove all MirrorView SRA Protection Side Array Managers.
 - f. Click **Close** to close the Configure Array Managers window.
5. If you configured array managers on the recovery side SRM server, follow step 4 to remove the array managers.
6. Run the installer **EMC_MirrorView_Site_Recovery_Adapter-1.x.y.z.exe**, where *x.y.z* specifies the version number on both protected and recovery SRM servers, to upgrade the adapter to the latest version.
7. On both protected and recovery SRM servers, restart the VMware Site Recovery Service by selecting **Start > Settings > Control Panel > Administrative Tools > Services**.
8. Configure the array managers and recreate the protection groups and recovery plans.

Installing the MirrorView Adapter

1. Install the MirrorView Adapter plug-in on both the protected and recovery SRM servers as follows:
 - a. Run the installer **MirrorView Site Recovery Adapter-1.x.y.z.exe**, where *x.y.z* specifies the version number.

If the installer does not find **.Net Framework** on an SRM server, it installs **.Net Framework** on the server.
 - b. Restart the VMware Site Recovery Service by selecting **Start > Settings > Control Panel > Administrative Tools > Services**.
2. When the installation of the MirrorView Adapter plug-in is complete on both the protected and recovery SRM servers, launch the VI Client on the protected site VirtualCenter Server.
3. On the toolbar, click **Site Recovery**, and connect the protected and recovery sites as described in the *VMware Site Recovery Manager Administration Guide*.
4. On the toolbar, click **Site Recovery**, and connect the protected and recovery sites as described in the *VMware Site Recovery Manager Administration Guide*.

If you see the following exception when you select the Site Recovery option while trying to connect the sites —

```
Exception has been thrown by the target of an invocation.
```

— verify that the VirtualCenter Servers point to a DNS server and are connected to the DNS domain.

5. When the sites are connected, configure the array managers for the CLARiiON storage systems as follows:
 - a. Using the VI Client, log in to the protected site VirtualCenter Server.
 - b. On the toolbar, click **Site Recovery**.
 - c. On the **Summary** tab, in the Setup pane, click **Configure** for the array managers.

- d. In the Protection Site Array Managers screen, click **Add**.
If you get the following error immediately after clicking **Add** during the array configuration procedure —
Unable to find any array script files. Please check your SRM installation.
— then at both sites either reboot the VirtualCenter Servers or restart the VMware Site Recovery Manager servers.
- e. In the Add Array Managers dialog box, enter the following information for the primary storage system (one at the protected site):
 - Display name – Name you want for the primary storage system
 - Manager type – Click the arrow and select **EMCMirrorView SRA**.
 - Storage processor – IP address of a storage processor in the primary storage system.
 - Username – Username for logging in to the storage processor.
 - Password - Password for the username.
- f. Click **Connect**.
- g. After the connection completes, click **OK**.
- h. When the storage system is visible in the Protection Arrays pane in the lower right, click **Next**.
- i. On the Recovery Site Array Managers screen, click **Add**.
- j. In the Array Managers dialog box, enter the following information for the *secondary* storage system (one at the recovery site):
 - Display name – Name you want for the secondary storage system
 - Manager type – Click the arrow and select **EMCMirrorView SRA**.
 - Storage processor – IP address of a storage processor in the secondary storage system
 - Username – Username for logging in to the storage processor.
 - Password - Password for the username.
- k. Click **Connect**.
- l. When the connection is complete, click **OK**.

- m. On the Recovery Site Array Management screen, when a green check mark appears next to the storage system in the Protection Arrays pane in the lower right, click **Next**.
- n. On the Review Replicated Datastores screen, click the plus sign next to the storage system, and review the tree to verify that the correct LUNs for the protected VMs are mirrored to the secondary storage system.

If the mirror images are not correct, click **Rescan Arrays** to correct the problem.

To see replicated datastores, the datastore must reside on a mirrored LUN and contain at least one VM.

- 6. Set up inventory mappings and protection groups as described in the *VMware Site Recovery Manager Administration Guide*.

Troubleshooting and getting help

EMC support, product, and licensing information can be obtained as follows.

Product information: For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Powerlink® website (registration required) at:

<http://Powerlink.EMC.com>

Technical support: EMC and VMware have cooperative support agreements to ensure that support requests are triaged and routed to the most appropriate support organization. We anticipate that most issues experienced in a VMware-SRM managed site failover will be exposed to you through the VMware SRM console and that the appropriate first contact for resolution of the issue will be the VMware SRA solution provider. This provider will triage the issue and either resolve the underlying root cause or engage the technology vendor, who the provider believes can correct the problem based on the triage findings.

EMC is the provider of the replication adapters that interface with the VMware SRM solution. EMC provides full support for these adapters and their corresponding replication solutions. If you see error messages in an EMC replication product or adapter log file that do *not* appear related to the VMware SRM product, you should contact EMC Technical Support as you normally would.

For technical support, go to EMC Customer Service on Powerlink. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Copyright © 2008-2009 EMC Corporation. All Rights Reserved.

EMC believes the information in this publication is accurate as of its publication date. However, the information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the Technical Documentation and Advisories section on EMC Powerlink.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.