

**EMC<sup>®</sup> MirrorView<sup>™</sup> Enabler  
for EMC VNX<sup>®</sup> SRA**

**Version 5.0.23**

**Release Notes**

**P/N 300-012-686  
Rev 04**

**September 2012**

---

These release notes contain supplemental information about EMC<sup>®</sup> MirrorView<sup>™</sup> Enabler for EMC VNX<sup>®</sup> SRA. Topics include:

♦ Revision history .....	2
♦ Product description .....	2
♦ New features and changes .....	2
♦ Fixed problems .....	3
♦ Environment and system requirements .....	3
♦ Technical notes .....	4
♦ Documentation .....	4
♦ Software media, organization, and files .....	5
♦ Installation and setup .....	5
♦ Troubleshooting and getting help .....	7

## Revision history

Revision	Date	Description
A01	November 2011	General availability of the product
A02	June 2012	Improvements to the Array Manager and bug fixes
03	July 2012	Improvements to LUN failovers
04	September 2012	64-bit support for SRM 5.1

## Product description

The EMC VNX SRA for VMware vCenter™ Site Recovery Manager 5 (VNX SRA) is a software package that enables VMware vCenter Site Recovery Manager (SRM) to implement disaster recovery for VMware® ESX™ server virtual machines by using EMC storage platforms.

The EMC MirrorView Enabler for EMC VNX SRA (MirrorView Enabler) specifically enables the VNX SRA to manage EMC VNX and EMC CLARiiON® systems during disaster recovery.

EMC MirrorView Insight for VMware (MVIV) is not applicable to the MirrorView Enabler and will not be maintained. EMC Solutions Enabler is not required. The EMC SRA MirrorView Enabler automatically creates and removes snapshots for test-failover, recovery, and reprotection workflows in SRM 5.

## New features and changes

The following are new features and changes.

- ◆ 5.0.23 release:
  - Supports VMware vCenter SRM 5.1, which supports 64-bit operating systems.

- ◆ 5.0.22 release:
  - When running a recovery, MirrorView Enabler creates a read-only storage group on the primary array into which the LUNs being failed over are added. MirrorView Enabler creates this read-only storage group to identify which hosts need access if the recovery fails. Beginning with MirrorView version 5.0.22, these read-only groups are removed during the reprotect phase, after verifying the success of the recovery.
  - No snapshot is created at the protected site during SRM recovery.
  - When adding LUNs to the storage group, the available HLU (Host Logical Unit) numbers are correctly identified.
  - Updated support for the CLARiiON AX4 by fixing the following:
    - SnapView commands no longer fail for LUNs on SPB because the code determined the SP ownership of the LUNs for AX4.
    - Fixed the parsing error for the SnapView Listsessions command.
- ◆ 5.0.17 release:
  - When you create an Array Manager, you can now enter a filter string that allows you to narrow the results of the list of discovered devices.
  - When adding an Array Manager, the field **Secondary Management IP/Hostname (MirrorView)** is now required.

## Fixed problems

There are no fixed problems in this release.

## Environment and system requirements

The VMware environment at both the protected (primary) and recovery (secondary) sites must meet the following requirements.

- ◆ The appropriate versions of VMware vCenter Server and VMware vCenter SRM are installed:
  - 32-bit systems — VMware vCenter Server 5.0 and VMware vCenter SRM 5.0
  - 64-bit systems — VMware vCenter Server 5.1 and VMware vCenter SRM 5.1

- ◆ MirrorView is configured correctly for SRM to facilitate disaster recovery operations.
- ◆ VMware vCenter SRM server is installed with the following:
  - VNX SRA
  - Navisphere Secure CLI
  - MirrorView Enabler

The server can be a vCenter server or a Windows host, and it must have one or more VMware ESX 4.1 U1, ESXi 5.0, or ESXi 5.1 servers connected to an EMC platform.

Navisphere® Secure CLI is required to install EMC SRA MirrorView Enabler. The Navisphere Secure CLI is available for download at <https://support.emc.com>.

**Note:** When installing Navisphere Secure CLI, select the **Include Navisphere CLI in Environment Path** option.

After installing or reinstalling Navisphere Secure CLI, restart the VMware Site Recovery Manager service.

- ◆ SnapView is installed on both the primary and secondary arrays.

## Technical notes

The VNX SRA and MirrorView Enabler allow VMware vCenter SRM to automatically drive the setup, testing, and failover portions of the disaster recovery processes for EMC VNX and CLARiiON platforms. The *VMware vCenter Site Recovery Manager Administration Guide*, available on the VMware website, provides more information.

## Documentation

Part number	Description
300-012-686	EMC MirrorView Enabler for VNX SRA Release Notes

Documentation for VMware vCenter Site Recovery Manager can be found at [http://www.vmware.com/support/pubs/srm\\_pubs.html](http://www.vmware.com/support/pubs/srm_pubs.html).

## Software media, organization, and files

The following table lists the installation files for MirrorView Enabler.

File name	Description
EMC_Mirrorview_Enabler_for_VNX_SRA_v5.0.23.exe	Installer for EMC MirrorView Enabler for EMC VNX SRA 5.0.1 – 32 bit
EMC_Mirrorview_Enabler_for_VNX_SRA_v5.0.23_64bit.exe	Installer for EMC MirrorView Enabler for EMC VNX SRA 5.0.1 – 64 bit

## Installation and setup

Before installing the MirrorView Enabler, install the VMware vCenter SRM server and VNX SRA on a supported host at both the protected and recovery sites. Make sure all environment and system requirements have been met as previously described.

### Install the MirrorView Enabler

Complete the following steps to install the MirrorView Enabler on both the protected and recovery SRM servers:

1. Run the Navisphere Secure CLI installer.
2. Run the appropriate MirrorView Enabler installer.
3. After the MirrorView Enabler is installed on the protected and recovery SRM servers, launch the vSphere Client for the protected site vCenter server.
4. Click **Site Recovery** in the **Solutions and Applications** section of the **vSphere Client** home page.
5. Connect the protected and recovery sites as described in the *VMware vCenter Site Recovery Manager Administration Guide* from VMware.
6. Set up inventory mappings and protection groups as described in the *VMware vCenter Site Recovery Manager Administration Guide*.
7. Click **Array Managers** on the bottom of the left pane.
8. For each site, click the **SRA** tab in the right pane.

9. Click the **Reload SRAs** link.
10. Create Protection Groups and Recovery Plans, as outlined in the *Administration Guide for Site Recovery Manager*.

### Storage requirements for using EMC VNX SRA 5.0.1 with MirrorView Enabler 5.0.x

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. Do the following 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. On the secondary storage system, create a matching destination LUN.
  - c. On the primary storage system, create a mirror containing the primary LUN and the secondary LUN that you just created.
4. On the primary storage system, create a consistency group that contains all the mirrors for the virtual machine.

**Note:** If the virtual machine uses only one LUN, a consistency group is not necessary.

### Upgrading from VMware vCenter SRM 4.x with MirrorView SRA 1.4

If you use the MirrorView SRA 1.4, the following configuration steps are no longer required:

- ◆ Assigning the destination LUN to the storage group for the recovery ESX Server host.
- ◆ Creating a SnapView snapshot of the source LUN and assign it to the storage group for the protected ESX Server host.
- ◆ Creating a SnapView snapshot of the destination LUN and assign it to the storage group for the recovery ESX Server host.

These snapshots were created with the same name as the base LUN, plus the suffix “\_VMWARE\_SRM\_SNAP” (. “LUN1 and LUN1\_VMWARE\_SRM\_SNAP”).

These snapshots are no longer used by the current SRA, as the snapshots are created as needed by the SRA. To delete the snapshots from a known good configuration, where the source LUNs are accessible from the protected ESX Server host(s), perform the following steps for each LUN for virtual machines that SRM is protecting:

1. On the primary storage system, remove the SnapView snapshot <LUN\_name>\_VMWARE\_SRM\_SNAP from the storage group and delete the snapshot.
2. On the secondary storage system, remove the SnapView snapshot <LUN\_name\_MIRROR>\_VMWARE\_SRM\_SNAP from the storage group and delete the snapshot.
3. Optional: On the secondary storage system, remove the destination LUN from the storage group for the recovery ESX Server host.

**Note:** The LUN is added (if not present) to the storage group when running a recovery through VMware vCenter SRM.

## 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 <https://support.emc.com>.

**Technical support:** For technical support, go to the EMC Service Center at <https://support.emc.com>. To open a service request, 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.

For more details on configuration and best practices with SRM, refer to the documents available at <https://support.emc.com>.

The history logs can be used for diagnostics and are located at C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs\SRAs\EMC VNX SRA.

Copyright © 2012 EMC Corporation. All rights reserved. Published in the USA.

Published September 2012

EMC believes the information in this publication is accurate of its publication date. 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.

EMC2, EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to the technical documentation and advisories section on the EMC online support website.