Violin Storage Replication Adapter User Guide

Document Number: 535-0236-00 Rev 01
October 2015

Violin Storage Replication Adapter User Guide

Version 5.11

LEGAL NOTICE

Violin Memory, Inc.
4555 Great America Parkway
Santa Clara, CA 95054
USA

Contents

Introduction

The Storage Replication Adapter (SRA) integrates with VMware vCenter Site Recovery Manager (SRM) to automate disaster recovery for systems using VMware Infrastructure with storage managed by Violin Concerto OS 7, built on Violin technology.

In a typical environment, there will be two sites: the protected site (the primary production site) and the recovery site. At each site, there will be a Concerto controller to manage storage for the host machines. In addition, the Concerto controller will replicate data from the protected site to the recovery site.

When a disaster occurs and the protected site is not available, the recovery plan can be run so that the system will fail over to the controller at the recovery site and the replicated data can be used.

For disaster recovery planning purposes, you can test your recovery plan through SRM. Testing can be done at any time without any impact to your production environment.

Installation

Requirements

Violin Storage Replication Adapter (SRA) must be installed with each instance of VMware vCenter Site Recovery Manager (SRM), at the protected site as well as the recovery site. SRA must be installed on the same host where SRM is installed.

Procedure

To install SRA:

1. Run the installation executable `SRA-5.11-<Build>.exe`

   If SRM is not detected, the installer will not proceed.

2. Follow the on-screen instructions to complete the installation wizard.

   SRA is installed under the installation folder of SRM.

   For example, if SRM is installed to its default location:

   ```
   C:\Program Files\VMware\VMware vCenter Site Recovery Manager
   ```

   SRA will be installed under:

   ```
   C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra\Violin
   ```

3. After installation completes, connect to SRM using the vSphere Client.
4. Navigate to the *Array Managers* screen and select the *SRAs* tab and make sure the correct version of SRA is present in the list.
   If it is not, click *Rescan SRAs* to refresh the list.

Configuration

Storage Replication Adapter (SRA) works within the framework of VMware vCenter Site Recovery Manager (SRM). Therefore, you should refer to the *VMware vCenter Site Recovery Manager Administration Guide* for general instructions on how to set up and configure virtual machines for protection.

This section details the storage-specific steps to be performed as part of the general SRM configuration process.

Configure Concerto Controllers to protect data

You must configure your Concerto controllers to protect your data by replicating virtual devices from the protected site to the recovery site and enabling snapshots on the devices. This is done through the Violin Symphony. The following is an overview of the steps that must be performed. Refer to the *Violin Concerto 7000 User's Guide* for detailed instructions.

1. Under the servers on the protected site, configure each ESX host as a SAN Client and assign virtual devices to it.
2. Configure replication for each virtual device that you want to protect.
3. Select a server on the recovery site as the replication target.
4. Under the server on the recovery site, configure each recovery host as a SAN Client.
5. Enable MemSnap for each primary device on the protected site, and each replica device on the recovery site.

Configure Array Managers in SRM

To configure SRM to use your Concerto controllers, you must add Array Managers on both the protected and the recovery sites.

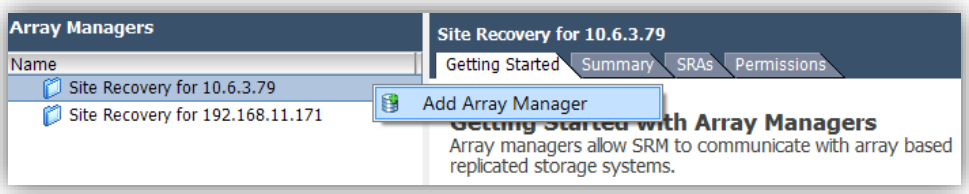
Overview

- Each array manager is defined as a pair of Concerto controllers, designated as *Local Storage Server* and *Peer Storage Server*, with a replication relationship in one or both directions between them.
- When adding an array manager at the protected site, enter the protected site controller as the *Local* server and its replication peer at the recovery site as the *Peer* server.
- Each array manager at the protected site must have a corresponding array manager defined at the recovery site.
- When adding an array manager at the recovery site, enter the recovery site controller as the *Local* server and its replication peer at the protected site as the *Peer* server.

- Each unique pair of replication peers must be entered as a separate array manager.

Procedure

1. Connect to SRM using the vSphere Client and navigate to the *Array Managers* screen.
2. Right-click on the name of the protected site in the left pane and select *Add Array Manager*.



3. Enter a display name for the array manager and select the appropriate SRA from the drop-down menu.

   Each array manager is defined as a *pair of Concerto controllers*, one at the local site and one at the remote site, that have a replication relationship between them. It is recommended that you select a display name that clearly identifies the server pair you are going to enter.
   For example: "Site A Server 1 > Site B Server 1"

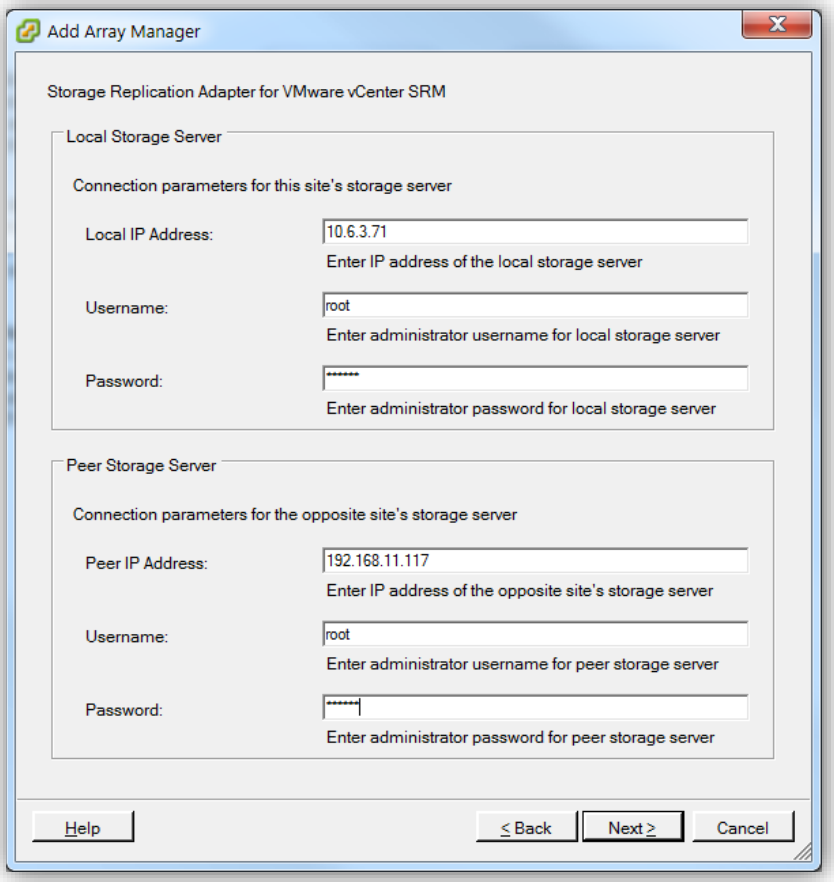
4. Enter the IP addresses and login credentials for the two Concerto controllers.

   Make sure the usernames you enter have administrative rights on the Concerto controllers.

   Note: When adding an array manager under the protected site, enter the details of the protected site Concerto controller under the *Local Storage Server* section, and enter the details of the recovery site Concerto controller under the *Peer Storage Server* section.

5. Click *Next* to add the array manager.

   The *Add Array Manager* screen displays.



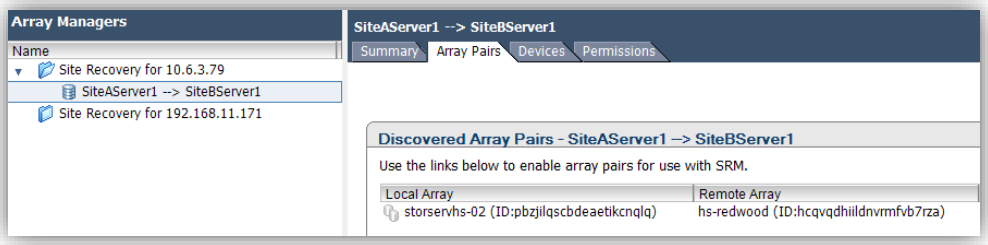
SRM then invokes SRA to discover the replication configuration of the server pair you entered on the previous screen. This may take several seconds depending on the total number of devices on the local storage server.

6. When discovery is complete, click *Finish*.

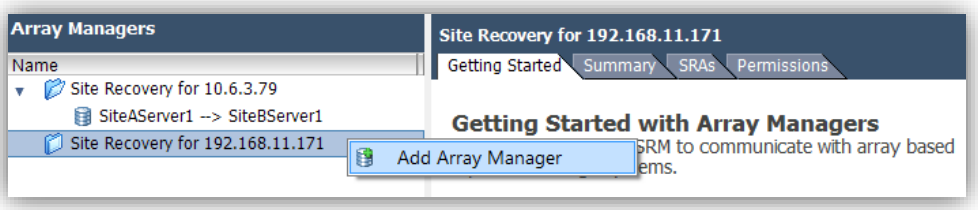
   The array manager you just added now appears under the protected site.

7. Click the array manager and the *Array Pairs* tab to view the discovered pair of storage servers.

   Each server is identified by its hostname, along with a unique ID that identifies the other server in the pair.



8. Now add a corresponding array manager under the recovery site by right-clicking on the name of the recovery site in the left pane and clicking *Add Array Manager*.



9. Enter a display name for the array manager and select the appropriate SRA from the drop-down menu.

   The server pair you enter here must be the same as the one you entered on the protected site (in Steps 3-4), but with the *Local* and the *Peer* servers reversed. Select an appropriate display name that reflects this.

   For example: "Site B Server 1 > Site A Server 1"

10. Enter the IP addresses and login credentials for the two Concerto controllers. Make sure the usernames you enter have administrative rights on the Concerto controllers.

    The server you enter under the *Local* section must be the same as the one you entered under the *Peer* section in Step 4. Similarly, the server you enter in the *Peer* section here must be the same as the one you entered in the *Local* section on the protected site.

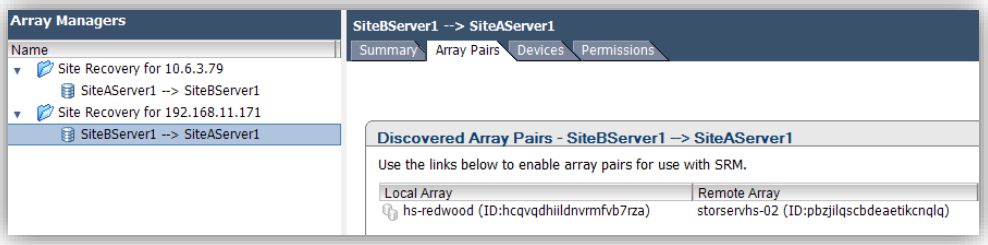
    Note: When adding an array manager under the recovery site, enter the details of the recovery site Concerto controller under the *Local Storage Server* section, and enter the details of the protected site Concerto controller under the *Peer Storage Server* section.

    SRM now invokes SRA to discover the replication configuration of the server pair you entered on the previous screen. This may take several seconds depending on the total number of devices on the local storage server.

11. When discovery is complete, click *Finish*.

12. Click on the newly-added array manager and the *Array Pairs* tab to see the list of discovered pair of storage servers.

    Note: The local array discovered here is the same as the remote array discovered on the other site, and the remote array here is the same as the local array on the other site.



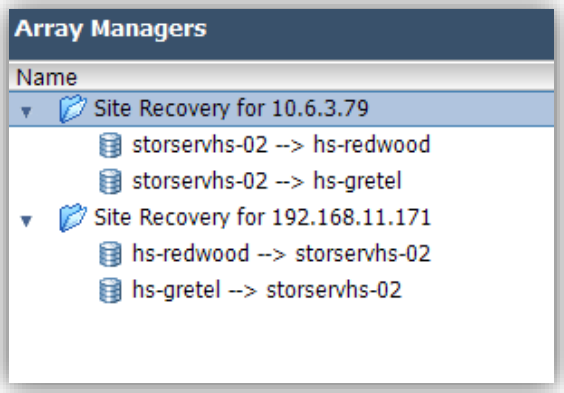
Configuring multiple pairs

If you have multiple storage servers on either site, you must enter each unique replication pair as a separate array manager.

For example, if `SiteAServer1` replicates a few of its devices to `SiteBServer1` and other devices to `SiteBServer2`, you must configure two array managers on Site A: one for each of the two replication pairs.

You will then need to add two corresponding array managers configured in the reverse direction on Site B.

The screen below shows an example of what your array managers should look like in such a case. The protected site server `storservhs-02` replicates some of its devices to the recovery site server `hs-redwood`, and other devices to the recovery site server `hs-gretel`.



Configuration Best Practices

- If you use Violin Memory Snapshot Director with SRM, you must configure Snapshot Director to skip the creation of VM snapshots during snapshot operations. SRM does not support failover/failback of virtual machines that have one or more VM snapshots present.

  Refer to the *Advanced Options* section of the *Snapshot Director User Guide* for instructions.

- Configure SRM to increase the default value of the timeout for certain operations.

  In the vSphere Client, navigate to the *Sites* screen, right-click on each site and then select *Advanced Settings*. Under the *storage* view, change the value of `storage.CommandTimeout` to `1800`. Under the *StorageProvider* view, change the value of `StorageProvider.HostRescanTimeoutSec` to `600`.

  You must set these values for the protected and the recovery sites.

- Make sure the replicated virtual devices on the storage server are either standalone or part of a replicated group. SRA does not support replicated virtual devices placed into non-replicated groups.

- If you enter hostnames instead of IP addresses when adding array managers, make sure all hostnames can be resolved on each SRM server, and on each storage server. It is very important that you use consistent capitalization for hostnames while configuring array managers. For example, do not enter the hostname as “MyProtServer” on one site and “MYPROTSERVER” on the other. Instead, use the exact same name on both sites.

Failover & Failback

This chapter outlines the steps you must perform to execute a failover or failback. Before you can do this, you must configure inventory mappings between your SRM sites, and create protection groups and recovery plans. Refer to your *SRM Administration Guide* for detailed instructions.

Test a recovery plan

For disaster recovery planning purposes, you can easily test your recovery plan through SRM. Testing can be done at any time without impacting your production environment, and while normal replication continues.

To test a recovery plan:

1. Select the recovery plan in SRM and click *Test Recovery Plan* to execute the recovery plan in test mode.

   During a test, SRA creates MemClones from the latest point-in-time snapshots of the relevant replicated devices on the recovery site Concerto controller and assigns them to the recovery host(s). SRM locates these newly attached devices and imports the virtual machines on them.

2. When testing is complete, click *Cleanup* under the recovery plan.

   This ends the test and notifies SRA to unassign the temporary MemClones from the recovery host(s) and delete them.

   Note: If the cleanup operation is interrupted or if an error occurs, MemClones may remain assigned to the recovery host. If this happens, you can manually unassign and delete the MemClones using Violin Symphony.

Run a recovery plan

In the event of a disaster, or a planned migration, you can run the recovery plan to failover virtual machines from the protected site to the recovery site. To run a recovery plan:

1. Select the recovery plan in SRM and click *Run Recovery Plan*.
2. Depending on whether the protected site is online, select the appropriate option for a planned migration or a disaster recovery.

   If the protected site is online, SRM shuts down the protected virtual machines and SRA synchronizes replication to make sure the replica devices are up-to-date. If synchronization is not possible, the latest image of the replica devices on the recovery site is used for recovery.

   SRA suspends replication for the relevant devices, promotes the devices on the recovery site and assigns them to the recovery host(s). SRM finds these newly attached devices and imports the virtual machines on them.

Note: If a recovery plan is interrupted or if there are errors for some storage devices, you can safely retry running the plan. SRA will ignore storage devices that have already been failed over, and will attempt to complete the failover for other devices.

Post Recovery

After you run a recovery plan, you will need to re-protect your data. You will notice the following changes:

- Your original protection groups and recovery plans are marked as invalid and are no longer usable to perform a failover.
- On the recovery site Concerto controller, the original replica devices are now promoted SAN Resources and are assigned to the recovery ESX hosts.

  The replication status on the newly promoted devices on the recovery site indicates that replication is in DR mode.
- On the protected site Concerto controller, the replication status on the original protected devices is marked as inactive.

Post recovery protection

You must repair your recovery plans and re-establish replication from the active recovery site back to the original protected site. Before you do this, make sure you have repaired your protected site and that it is fully functional.

To re-protect, select the recovery plan in SRM and then click *Re-protect*.

SRM invokes SRA to re-establish replication back to the original protected site. As part of this step, SRA will un-assign the original source devices (that are no longer in use) from all SAN Clients on the original protected Concerto controller.

SRA will also repair the replication configuration so that the newly promoted devices on the recovery site begin to replicate data back to replica devices on the original protected site.

As part of this step, SRA will restore the replication schedule that was originally configured on these devices. If continuous replication was configured, SRA will also re-enable this setting.

SRM repairs your protection groups and recovery plans so that they now establish protection in the opposite direction. This means the failed-over virtual machines on the recovery site are now placed in protection groups, and the original protected site now contains recovery plans that can be run to perform a failback.

Note: If the re-protect operation is interrupted or if there are errors for some storage devices, you can safely retry the operation. SRA will ignore storage devices that have already been repaired, and will attempt to re-establish replication for all other devices.

Failback

When you use the *Re-protect* option as described in the previous section, SRM automatically reconfigures your protection groups and recovery plans to establish protection in the opposite direction. That is, from the recovery site to the original protected site.

When you are ready to failback to the protected site, simply test and run the recovery plan to perform a planned migration back to the protected site. When the migration is complete, perform a re-protect operation to re-establish the original protection to the recovery site.

Refer to the *SRM Administration Guide* for details.

Appendix A

Determining the SRA version

To see what version of Storage Replication Adapter (SRA) is installed on an SRM site, log in using the vSphere Client, navigate to *Array Managers*, and switch to the SRAs tab under the appropriate site. A summary of all SRAs installed is displayed here.

If this information is not available using the vSphere Client, run the `command.pl` Perl script under the SRA folder with the switch "-v" from the Windows Command Prompt.

For example:

```
> perl "C:\Program Files\VMware\VMware vCenter Site Recovery
Manager\storage\sra\Violin\command.pl" –v
```

Note: If perl is not in the PATH, you may need to enter the full path to the Perl.exe executable.

Sample output:

```
Violin Memory Storage Replication Adapter for VMware SRM
Version 5.11 (Build 5111)
```

Generating Checksums of installed files

You may need to compute MD5 hash checksums of certain installed files under the SRA folder when contacting Technical Support. To do this, download and install the Microsoft File Checksum Integrity Verifier Utility (available at http://support.microsoft.com/kb/841290).

Once installed, using the Windows command-line, run the `fciv` utility with the full path to the file whose checksum you want to compute. You may need to provide the full path to the `fciv` executable, or add it to the PATH environment variable. Refer to the utility's documentation for detailed usage instructions.

Generally, you will need to compute checksums for all of the Perl Module (.pm) files under the SRA installation folder's `lib` directory. For example, run the following commands to compute checksums of all modules at once and save the output to a text file:

```
> cd "C:\Program Files (x86)\VMware\VMware vCenter Site
Recovery Manager\storage\sra\Violin\lib"

> fciv *.pm > checksums.txt
```