

# Dell PowerVault MD Storage Array VMware Storage Replication Adapter (SRA)

## Installation and Configuration Manual

Regulatory Model: E16S Series  
Regulatory Type: E16S001



# Notes, Cautions, and Warnings



**NOTE:** A NOTE indicates important information that helps you make better use of your computer.



**CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



**WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

**Copyright © 2014 Dell Inc. All rights reserved.** This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2014 - 06

Rev. A09

# Contents

<b>1 Data Recovery Using VMware And Dell MD Storage Arrays.....</b>	<b>5</b>
SRM Overview.....	5
SRA Overview.....	6
<b>2 Setting Up Your Environment.....</b>	<b>7</b>
Installation Prerequisites.....	7
Compatibility Requirement.....	7
Remote Replication And Snapshot Premium Feature Activation.....	7
Protected And Recovery Site Installation Requirements.....	8
Dell MD Storage Array Installation Requirements.....	8
Virtual Disk Layout Considerations.....	8
Setting Up Remote Replication On The MD Storage Array.....	9
Host-To-Storage Array Configuration.....	9
Switch Zoning Requirements.....	10
<b>3 Installing The Recovery Solution Components.....</b>	<b>11</b>
About This Guide.....	11
Summary Of Tasks.....	11
Installing Supported Standalone Database.....	12
Installing vCenter Server.....	12
Installing Site Recovery Manager.....	12
Configure an ODBC Connection To Your Standalone Database.....	12
Installing SRM On The Protected and Recovery Site.....	12
Install The vCenter SRM Plug-in.....	12
Downloading And Installing The MD Storage Replication Adapter.....	13
Changing RAID Controller Passwords On The Storage Array.....	14
<b>4 Configuring The Recovery Solution.....</b>	<b>15</b>
Starting Site Recovery Manager.....	15
Using vSphere With Site Recovery Manager.....	15
Configuring Site Recovery Manager.....	16
Connect Recovery And Protected Sites.....	16
Set Up Inventory Mappings.....	17
Assign Placeholder Datastores.....	18
Configuring Storage Array Managers.....	19
Rescan And Enable The SRAs.....	20
Creating Protection Groups.....	21
Creating A Recovery Plan.....	21

<b>5 Testing And Running Recovery Plans.....</b>	<b>24</b>
Testing Recovery Plans.....	24
Running Recovery Plans.....	25
<b>6 Fallback Procedures.....</b>	<b>27</b>
<b>7 Troubleshooting and Miscellaneous Issues.....</b>	<b>28</b>
Rescan During Failover Not Detecting Virtual Disk Mappings.....	28
Removing The Snap-XXX- Prefix On Failed-Over Datastores.....	28
Debugging SRA Errors.....	28
<b>8 Reference Information.....</b>	<b>30</b>
Contacting Dell.....	30
Related Documentation (Other Information You May Need).....	30
VMware Support Information.....	31
Locating Your System Service Tag.....	31
Documentation Feedback.....	31

# Data Recovery Using VMware And Dell MD Storage Arrays

In an effort to consolidate and more efficiently use server resources, many applications formerly run in a dedicated physical server environment are being migrated to virtual machines (VMs) or virtual servers operating in a VMware ESX-based virtual infrastructure. Benefits of this migration away from single, dedicated server platforms, especially for production environments requiring high-performance, block-level storage, are:

- Higher availability
- Increased flexibility
- Scalability

VMware's vCenter Site Recovery Manager (SRM) offers a disaster recovery solution (DRS) using the Remote Replication feature of the Dell PowerVault MD storage array to provide automated failover of servers and VMs, as well as the underlying storage and datastores they use. This automated recovery solution is designed to both:

1. Provide lower-costs for tier-2 and tier-3 applications.
2. Introduce DRS to smaller businesses that generally do not require enterprise-class storage and services.

## SRM Overview



### NOTE:

The Dell PowerVault SRA can be used on MD Storage Arrays based on both Fibre Channel and iSCSI configurations.

For more information about supported versions of SRM and MD Storage Arrays, see the Support Matrix at [dell.com/powervaultmanuals](http://dell.com/powervaultmanuals).

SRM is a recovery workflow product that automates setup, failover or failback, reprotect and testing of recovery plans. SRM leverages the Dell MD storage array's block-based Remote Replication feature by using an MD-specific Storage Replication Adapter (SRAs), which is a set of hardware applications vendor to control replication of data from the primary site to the recovery site. The figure below shows that the hierarchical relationship of the database, operating system, VMware applications and storage array in the SRM architecture.

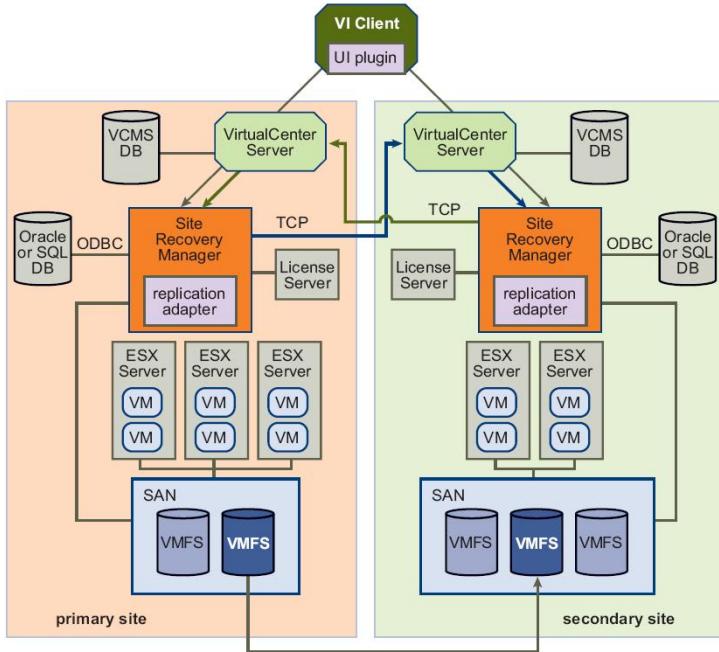


Figure 1. SRM Architecture

## SRA Overview

The MD-specific Storage Replication Adapter (SRA) interacts with the SRM to discover, replicate and when required, failover to the storage arrays between recovery sites. Also, the SRA interacts with the storage array to provide test failover capabilities to the SRM.

# Setting Up Your Environment

This section details initial setup requirements for using VMware vCenter Site Recovery Manager (SRM) and the Dell MD storage array-based Storage Replication Adapter (SRA).

## Installation Prerequisites

Implementing a successful recovery solution using VMware and the remote replication features of the Dell MD storage array requires specific installation and configuration tasks on the VMware application platform and MD storage array.

The following VMware platforms are required.

- ESX host server (connected to MD storage arrays)
- vSphere Client
- vCenter Server
- Site Recovery Manager (SRM)
- Storage Replication Adapter (SRA)

## Compatibility Requirement

 **NOTE:** For the latest supported software VMware versions for vSphere Client, vCenter Server, Site Recovery Manager, Storage Replication Adapter and firmware updates, see *PowerVault MD Series Support Matrix* on [dell.com/support/manuals](http://dell.com/support/manuals).

Before the installation, note the following compatibility requirement.

- vSphere Client and Site Recovery Manager (SRM) version must match with the version of vCenter Server that it is connecting to. If a different version of vCenter Server is found, it will prompt to download a new client from that vCenter Server.

 **NOTE:** For information on installing these applications, refer to the VMware platform documentation at [vmware.com/support/product-support](http://vmware.com/support/product-support).

## Remote Replication And Snapshot Premium Feature Activation

SRA requires that these Dell MD storage array premium features be activated on each array used in your recovery solution:

- Remote Replication
- Snapshot Virtual Disk

For more information on obtaining and activating MD premium features, go to [dell.com/support](http://dell.com/support) and select your array model from the product selector.

## Protected And Recovery Site Installation Requirements

As part of configuring the recovery solution described in this guide, the required VMware platforms must be installed on both the protected (primary site) and recovery (secondary site) host sites. For more information, see *Installing the Recovery Solution Components*.

## Dell MD Storage Array Installation Requirements

SRM relies on the MD storage array's Remote Replication premium feature to maintain data replication between the protected site and the recovery site. Replication must be configured on the MD storage array before configuring SRM. See the corresponding Deployment Guide for your storage array at [dell.com/support/manuals](http://dell.com/support/manuals).

## Virtual Disk Layout Considerations

Before setting up Remote Replication, consider the datastores residing on the virtual disk as well as the virtual machines residing on the datastore. Remote Replication on the MD storage array functions on a virtual disk-level only; therefore, any datastores or virtual machines residing on a replicated virtual disk are protected. If no virtual machines require protection, make sure that your virtual machines-to-datastores-to-virtual disks are designed efficiently. For example, in the figure Single Virtual Disk Replication, a 400 GB virtual disk is used to house a single datastore containing four virtual machines. However, only VM1 and VM4 require protection. If a single virtual disk containing a single datastore is created, all four virtual machines will be protected, but at a cost of replicating 400 GB of data across the network link to a remote storage array.

Single Large Virtual Disk Replication

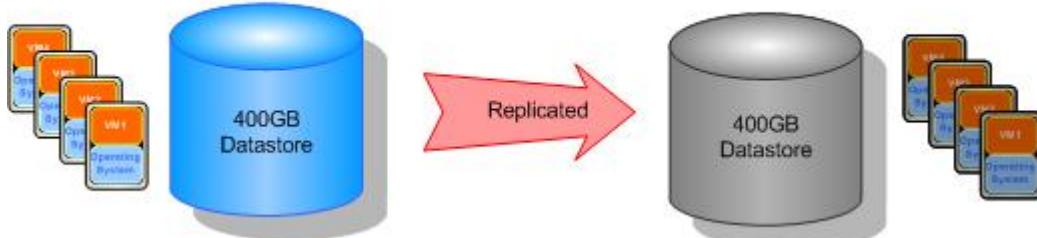


Figure 2. Single Virtual Disk Replication

Using the same protection requirements, figure Multiple Virtual Disk Replication shows that the multiple virtual disks created and only the virtual machines that require protection being replicated. The result is less data moving across the network, as well as increased ability to control individual failovers of VM1 or VM4, if necessary.

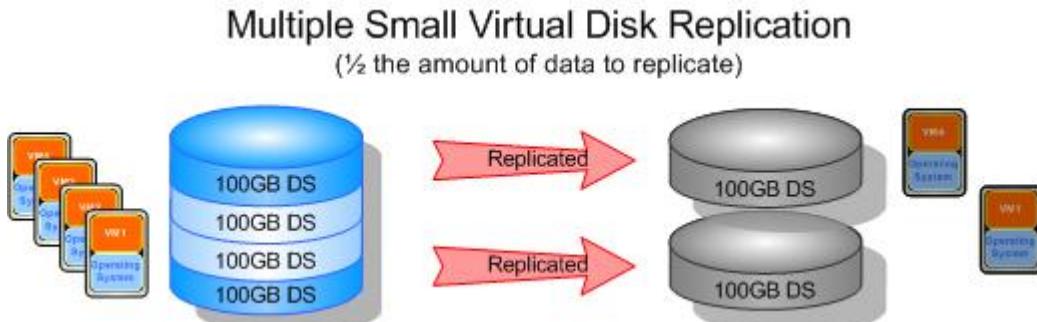


Figure 3. Multiple Virtual Disk Replication

## Setting Up Remote Replication On The MD Storage Array

**NOTE:** You must activate the Remote Replication premium feature before performing the steps below. For step-by-step instructions on using MD Storage Manager (MDSM) to set up Remote Replication, see the Administrator's Guide for your array at [dell.com/support/manuals](http://dell.com/support/manuals).

Before installing and configuring SRM, you must set up Remote Replication on each MD storage array used in the recovery solution.

**NOTE:** Setup of Remote Replication on iSCSI based PowerVault storage MD Series array is governed by iSCSI array documents available on [dell.com/support/manuals](http://dell.com/support/manuals).

To set up Remote Replication on the storage array:

1. Start **MD Storage Manager (MDSM)** on your management host.
2. Open the **Enterprise Management** Window (EMW) and discover both the protected and recovery site's storage array.
3. Open the **Array Management** Window (AMW) for the protected site's storage array and identify a virtual disk to be used in the recovery solution.
4. Open the **AMW** for the recovery site's storage array and create a similar-sized, remotely replicated virtual disk.
5. Right-click on the **protected site's storage array virtual disk** and select **Create Remote Replication**
6. Select the settings appropriate for your environment and allow remote replication to synchronize.
7. Repeat these steps for:
  - a. Each virtual disk to be remotely replicated
  - b. Each storage array in the recovery solution

## Host-To-Storage Array Configuration

To ensure optimal performance and proper multi-pathing for your configuration, the switch fabric and iSCSI connecting the protected and recovery host sites and the storage arrays must be properly configured. The following diagram illustrates a basic configuration that provides full redundancy:

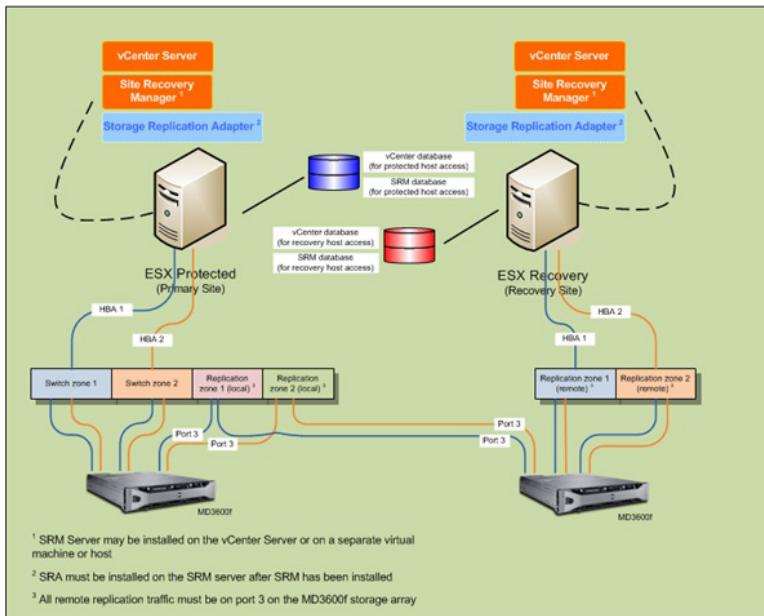


Figure 4. Fibre/iSCSI Channel Multi-path Configuration

## Switch Zoning Requirements

Switches used in a fibre-channel and iSCSI configuration must employ zoning. These switch zoning requirements must be observed:

- Each host bus adapter (HBA) on the host server must connect to a separate switch zone; no more than one HBA may be connected to one logical switch zone.
- Port 3 on each of the MD storage array controller is reserved for Remote Replication. This is required for fibre-channel only. iSCSI does not require any dedicated port.
- For fibre-channel, a separate zone must be created for each Remote Replication port.
- No more than four data paths (port-to-port segments) can be established from a single, physical host server to a single RAID controller.

For additional MD storage array zoning information, see the Deployment Guide for your array at [dell.com/support](http://dell.com/support).

For additional VMware-related zoning information, see *VMware Fibre Channel SAN Configuration Guide* at [vmware.com/support/product-support](http://vmware.com/support/product-support).

# Installing The Recovery Solution Components

The recovery solution described in this guide is based on the concept of a protected main site (host server or virtual machine) connected to an identically configured recovery site ready to take over should the protected site become unavailable. For this type of failover to be possible, both sites must have independent installations of the required recovery solution components. The procedures in this section guide you through the installation of these solution components on the protected site and the recovery site:

- A standalone database with a connection to both vCenter Server and SRM Server
- vCenter Server
- vSphere Client
- vCenter Site Recovery Manager (SRM)
- Storage Replication Adapter (SRA)

 **NOTE:** For more information, see [Compatibility Requirements](#) under Installation Prerequisites section of this document.

## About This Guide

This guide describes how to set up the recovery solution in vSphere, as well as how to configure certain SRM settings required by SRA to discover the MD storage arrays and recognize Remote Replication connections. However, it does not provide step-by-step instructions for installing VMware platforms. For complete installation information on these platforms, see the following VMware documentation:

- *VMware Site Recovery Manager Administration Guide*
- *VMware vSphere Installation and Setup Guide*
- *ESXi and vCenter Server Documentation Center at [vmware.com/support/pubs](http://vmware.com/support/pubs)*

 **NOTE:** To select appropriate VMware document based on the VMware versions, see the Compatibility Requirements document.

## Summary Of Tasks

These tasks represent a high-level view of the recovery solution installation and configuration process:

 **NOTE:** Each of these tasks must be completed separately on both the protected and recovery sites.

1. Install a supported database server and configure ODBC (Open Data Base Connectivity) connections.
2. Install vCenter Server
3. Install vSphere Client
4. Install SRM
5. Install the SRM Plug-in (in vSphere).

6. Install SRA on both vCenter SRM Servers.
7. In SRM, configure connections, set inventory mappings, assign datastores, configure array managers, create protection groups and recovery plans.
8. Test failover or failback between protected and recovery sites.

The following sections describe each task in more detail. Where indicated, refer to the VMware documentation to install non-Dell platforms.

## Installing Supported Standalone Database

Both vCenter Server and SRM Server require a standalone database to maintain environment-specific information. For smaller environments, vCenter Server can be installed with Microsoft SQL Runtime Server, which eliminates the need for an external database server. However, for larger environments, an external database is highly recommended. A list of supported database servers and configuration requirements are available in the *Site Recovery Manager Administration Guide*.

Once this standalone database is installed, a connection to SRM must be established. See *Installing Site Recovery Manager* for more information.

For detailed information on how to install and set up supported databases on vCenter Server and SRM, see *VMware Site Recovery Manager Administration Guide* at [vmware.com/support/pubs](http://vmware.com/support/pubs).

## Installing vCenter Server

Install vCenter Server on both the protected and recovery sites. For installation information, see *VMware vSphere Installation and Setup Guide* at [vmware.com/support/pubs](http://vmware.com/support/pubs).

## Installing Site Recovery Manager

 **NOTE:** Before installing SRM, make sure that you have installed a supported database as described in the *Installing Supported Standalone Database* section.

### Configure an ODBC Connection To Your Standalone Database

To configure an ODBC connection:

1. Go to the **C:\Windows\SysWOW64** directory.
2. Run the **odbcad32.exe** installer.

### Installing SRM On The Protected and Recovery Site

Install SRM on both the protected and recovery sites. For installation information, see *VMware Site Recovery Manager Administration Guide*.

### Install The vCenter SRM Plug-in

1. Once SRM is installed, start vSphere Client and connect to the installed vCenter Server.
2. From vSphere Client, select **Plug-ins** —> **Manage Plug-ins**.
3. From the **Plug-in Manager** window under **Available Plug-ins**, click **Download and Install** for the vCenter SRM Plug-in.
4. When the plug-in installation completes, close the window.

Make sure you install the vCenter SRM Plug-in on both the protected and the recovery site.

Once SRM is installed, the Site Recovery icon displays on the vSphere Client home page under Solutions and Applications. Use this icon to launch the SRM and configure your recovery solution with SRM.

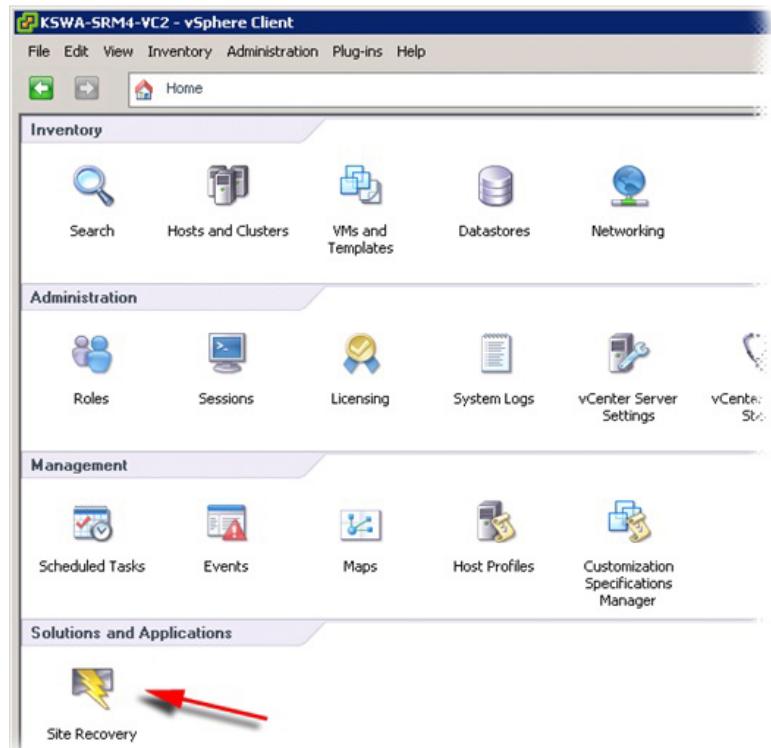


Figure 5. vSphere Site Recovery Manager

## Downloading And Installing The MD Storage Replication Adapter

SRA is available as a self-extracting, self-installing file from the Drivers and Download page at [dell.com/support](http://dell.com/support).

To download SRA:

1. Go to [dell.com/support](http://dell.com/support) and select **Drivers and Download**.
2. Use the Dell product selector to find your MD storage array model. Choose **Select Model** → **Servers, Storage & Networking** → **PowerVault Storage**.
3. Under **Select Your Product Model**, choose your MD storage array model.
4. Click **Confirm** to display available drivers and downloads for your MD storage array model.
5. Under **Applications**, choose the SRA download link.
6. Install the SRA executable using the installer included in the downloaded package.

 **NOTE:** Repeat steps 1 through 6 on both the protected and recovery site SRM Server.

## Changing RAID Controller Passwords On The Storage Array

The default SRA configuration assumes storage array passwords are not configured. If you need to use passwords on the storage arrays, modify the **SraConfigurationData.xml** file as described below:

1. Go to **C:\Program Files (x86)\VMware\VMware vCenter Site Recovery Manager\scripts\SAN\**Dell.
  2. Using a standard text editor, open the **SraConfigurationData.xml** file.
  3. Locate the `<!-- <PasswordRequiredForArrayAccess /> -->` line and change the false setting to true.
  4. Click **Save**.
-  **NOTE:** Support for mixed authentication types is not supported with the SRA. If any storage array within the SRM configuration has password authentication enabled, all other storage arrays will require password authentication. Passwords between storage arrays are not required to be the same.
5. Restart the vCenter SRM Server service from the services.msc console. This allows the SRM to detect the newly installed SRA and register any changes made to the **SraConfigurationData.xml** file.

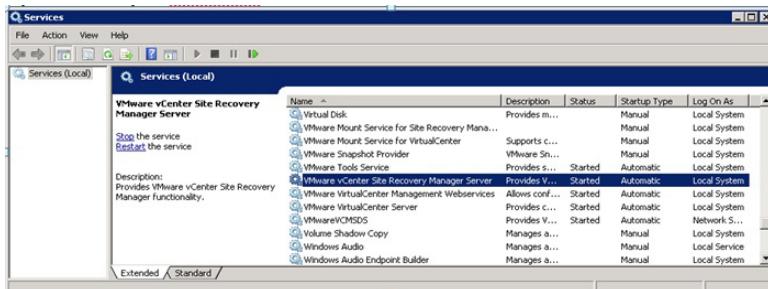


Figure 6. Viewing the Services.msc Console

# Configuring The Recovery Solution

Before configuring your recovery solution, make sure the following components have been successfully installed on both the protected and recovery sites:

- Supported database server with ODBC properly configured
- vCenter Server/vSphere Client
- Site Recovery Manager (SRM) (on physical or virtual machine)
- SRM vSphere Plug-in
- Storage Replication Adapter (SRA)

## Starting Site Recovery Manager

To begin configuring your recovery solution:

1. Start the **vSphere Client**.
2. Start Site Recovery Manager by clicking on the **Site Recovery** icon from the vSphere home screen.
3. Click the **Getting Started** tab to display the Getting Started with Site Recovery Manager screen.

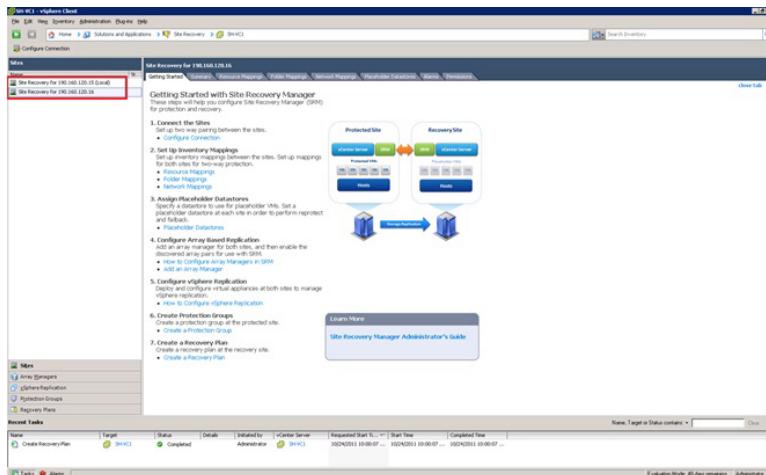


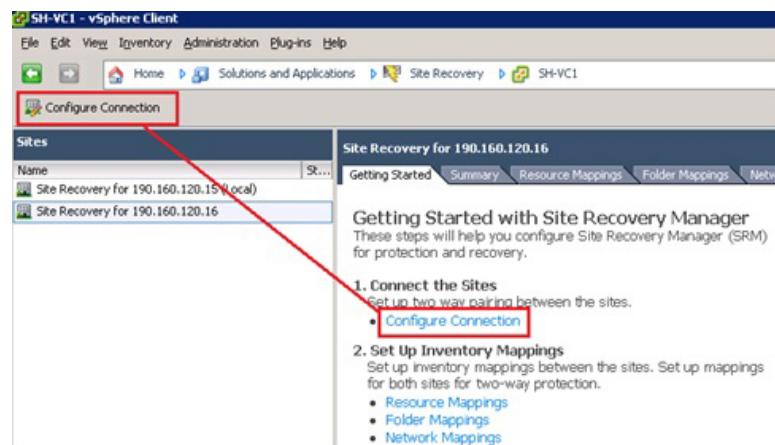
Figure 7. Site Recovery View in vSphere

**NOTE:** In the example screen above, the Sites pane shows the protected (190.160.120.15) and recovery (190.160.120.16) sites established previously when you installed vCenter. Do not continue with the steps shown in the section below until these installations are complete and are displayed in the vSphere view.

## Using vSphere With Site Recovery Manager

The **Getting Started with Site Recovery Manager** screen shows the basic steps required to configure SRM between the protected and recovery sites, as well as useful links to specific VMware documentation and online help. As you follow

the steps described in the following sections, you can return to this Getting Started page to launch specific configuration steps using the active page links, or use the drop-down menus available in the standard menu bar at the top of the page. Depending on the task you are performing, a command link may also be displayed at the top left of the screen.



**Figure 8. Selecting Configuration Tasks**

For more information, refer to *VMware vSphere Basics* at [vmware.com/support/pubs](http://vmware.com/support/pubs).

## Configuring Site Recovery Manager

Configuring your recovery solution consists of:

- Connecting the recovery and protected sites
- Setting up mapping to support two-way pairing
- Assigning a datastore at both protected and recovery sites to facilitate failover
- Configuring array managers
- Discovering array pairs for remote replication
- Enabling SRA
- Creating protection groups (on protected site)
- Creating a recovery plan (on recovery site)

### Connect Recovery And Protected Sites

To connect the protected and recovery sites:

1. Start **vSphere Client** and connect to the vCenter Server at the protected site.
2. Start **Site Recovery Manager** by clicking on the **Site Recovery** icon from the vSphere home screen.
3. From the **Getting Started** tab or the **Command** menu bar at the upper left, choose **Configure Connection**.
4. Enter the IP address or DNS name and port number for the remote vCenter Server, then click **Next**.
5. Enter administrator credentials for the vCenter Server on the recovery site and click **Next**.
6. Validate the SRM Certificate and click **OK**.
7. Review the SSL Security Warnings and install the certificates. Click **Ignore** to continue.

 **NOTE:** As the connection is made, green check marks are displayed next to each completed task in the wizard. If any tasks are marked as incomplete or failed, resolve the error status before continuing.

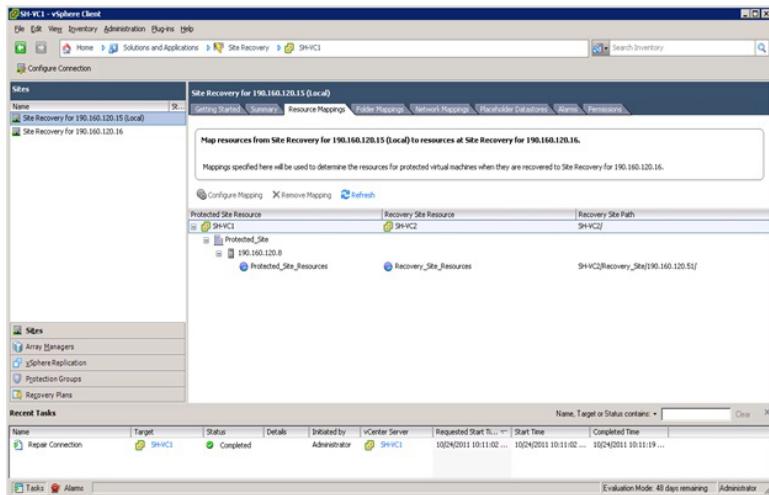
- Click **Finish** to complete the connections wizard.

Once these steps are complete, a two-way connection between the protected and recovery sites is established.

## Set Up Inventory Mappings

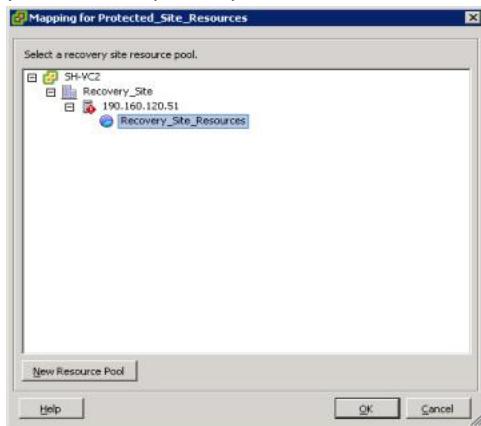
After making the connection between the protected and recovery sites, configure the resource, folder and network mappings necessary between the protected and recovery sites. These mappings provide default locations and networks used when placeholder virtual machines are initially created on the recovery site.

- Select the **Resource Mappings** tab.
- Select the **Configure Mapping**.
- Select the **Protected site** and click **Configure Mapping**.



**Figure 9. Resource Mapping View**

The mapping selection window is displayed. Expand the inventory items and navigate to the recovery site resource you want to map to the protected site resource.



**Figure 10. Mapping Selection Window**

- Click **OK** to complete the mapping.
- Repeat these steps for **Folder Mappings** tab and **Network Mappings** tabs, if desired.

Once complete, you will have established one-to-one mappings between the protected site's resources and the recovery site's resources.

## Assign Placeholder Datastores

For each virtual machine in a protection group, SRM establishes a placeholder at the recovery site to support failover and re-protection. As part of configuring the recovery solution, you must identify the datastore that SRM will use to store the placeholder data.

1. Click the Placeholder Datastores tab.

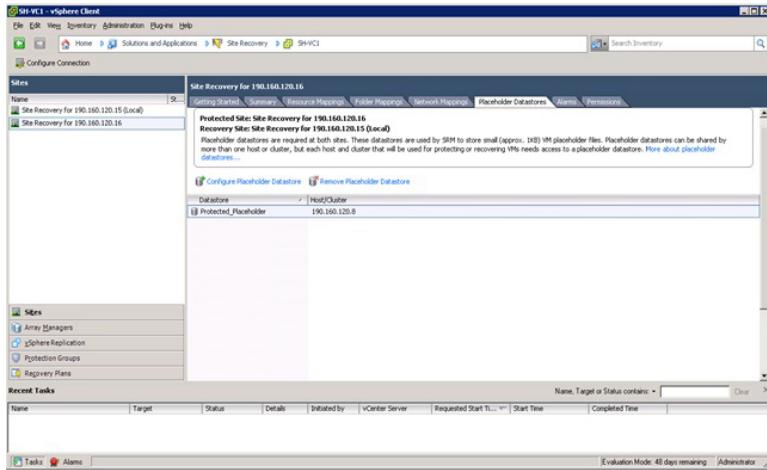


Figure 11. Placeholder Datastores Tab

2. Click Configure Placeholder Datastore.
3. In the placeholder datastore selection window, select **datastore** to support re-protect and failback.

**NOTE:** The placeholder datastore selected should be the highest enumerated LUN (generally LUN 0).

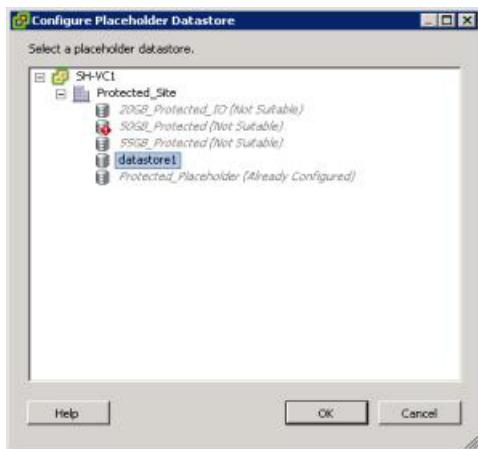


Figure 12. Placeholder Datastores

4. Click OK to finish the selection.

# Configuring Storage Array Managers

Once the protected and recovery sites are connected (for more information refer to the topic Connect Recovery and Protected Sites), the storage array managers on both sites must be configured so that SRM can discover remotely replicated data and devices, manage datastore groups and perform storage operations.

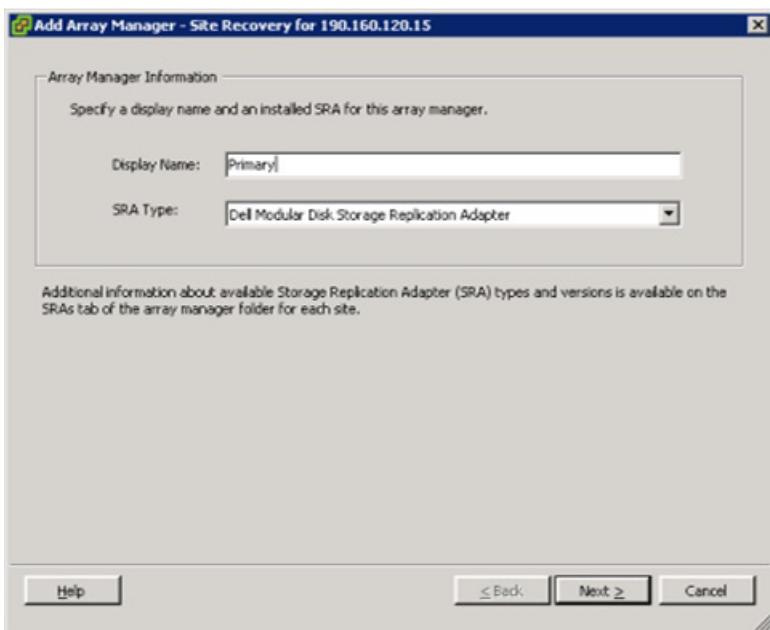
In this step, you will provide information to the storage array manager detailing:

- SRA type and display name
- Storage array connection information and passwords (if used) for both the protected and recovery sites

 **NOTE:** Typically, storage array managers do not need to be re-configured unless connection information, passwords or storage array components change.

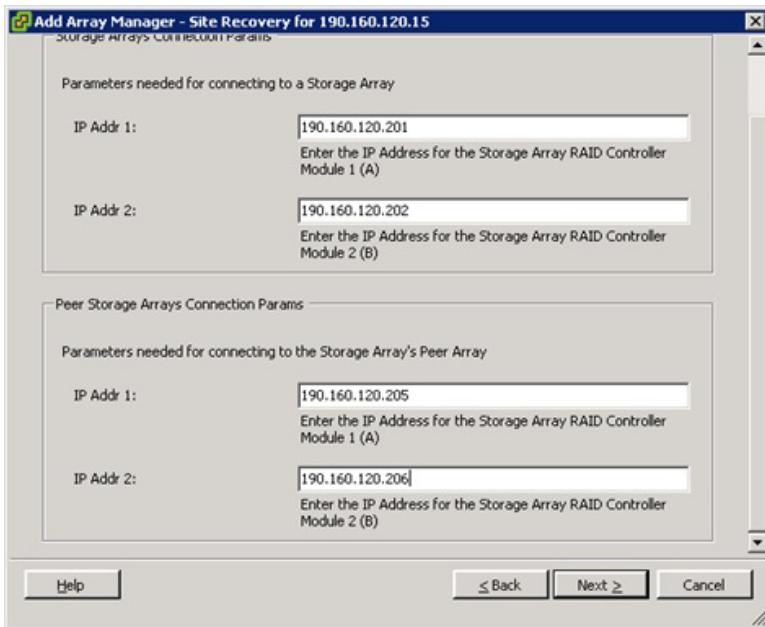
To configure the storage array managers on both sites:

1. From the **Getting Started** tab or **Array Managers** view, choose **Add an Array Manager**.



**Figure 13. Add Array Manager**

2. Enter the **Display Name** for the protected site's storage array. Then, click **Next**.
3. In the **Storage Arrays Connection Params** section:
  - a. For **IP Addr 1**, enter the IP address of the MD storage array's RAID controller 0.
  - b. For **IP Addr 2**, enter the IP address of the MD storage array's RAID controller 1.
4. In the **Peer Storage Arrays Connection Params** section:
  - a. For **IP Addr 1**, enter the IP address of the replicated MD storage array's RAID controller 0.
  - b. For **IP Addr 2**, enter the IP address of the replicated MD storage array's RAID controller 1.
5. If RAID controller passwords are enabled, you must also supply authentication.



**Figure 14. Array Manager Parameters**

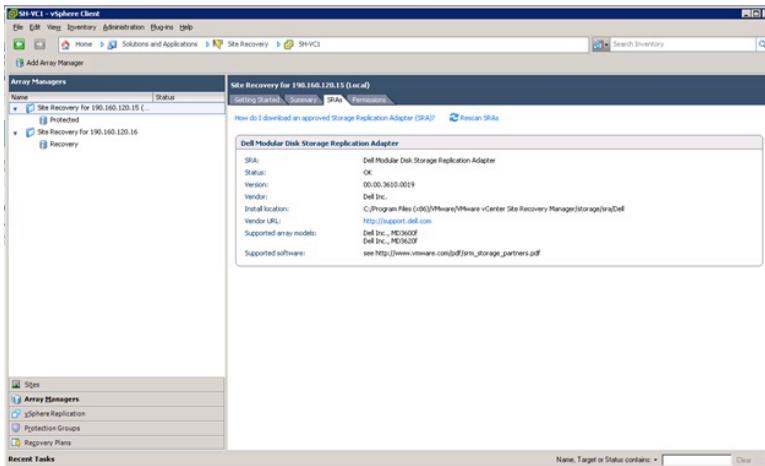
6. Click **Next** to validate the information and discover the storage arrays.
7. Click **OK** to complete the array manager configuration on the protected site.
8. Repeat these steps for the recovery site.

## Rescan And Enable The SRAs

Once the storage arrays on both the protected and recovery sites have been discovered:

1. From the **Array Managers** view, click the **SRAs** tab.

The SRAs tab should look similar to this:



**Figure 15. Array Managers View**

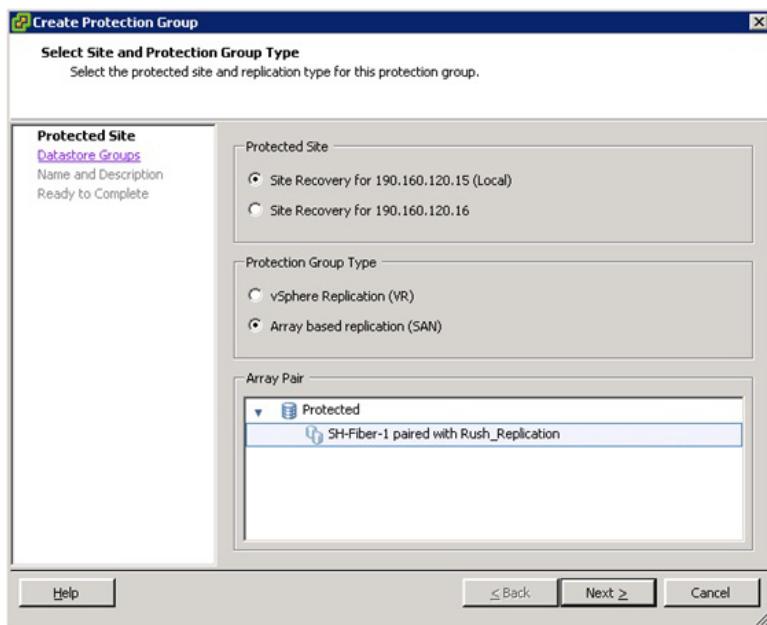
2. Select the **protected site** and click **Rescan SRAs**.

3. Select the **recovery site** and click **Rescan SRAs**.
  4. Select either the **Protected** or **Recovery** spindle in the **Array Managers** view.
  5. Select the **Array Pairs** tab.
  6. Click **Enable** to activate the SRA on both the protected and recovery sites.
- The SRAs should be loaded into SRM. Check the **Summary** tab to ensure that they display properly.

## Creating Protection Groups

The final configuration step at the protected site is to create Protection Groups for the VMs that you want to include in the recovery solution. SRM associates datastore groups with protection groups to collect any files related to virtual machine failover.

1. In **Protection Groups** view, select **Create Protection Group**.
2. In the **Select Site and Protection Group Type**, select the protected site.



**Figure 16. Creating a Protection Group**

3. In **Protection Group Type**, select the **Array based replication (SAN)** option.
4. Select one or more datastore groups from the list, then click **Next**.
5. Enter a name and optional description for the protection group, then click **Next**.
6. Click **Finish** to create the protection group.

## Creating A Recovery Plan

The final step in the solution configuration process is to create a recovery plan in the recovery site.

1. In **Recovery Plans** view, select **Create a Recovery Plan**.
2. In the **Recovery Site** window, choose the recovery site.

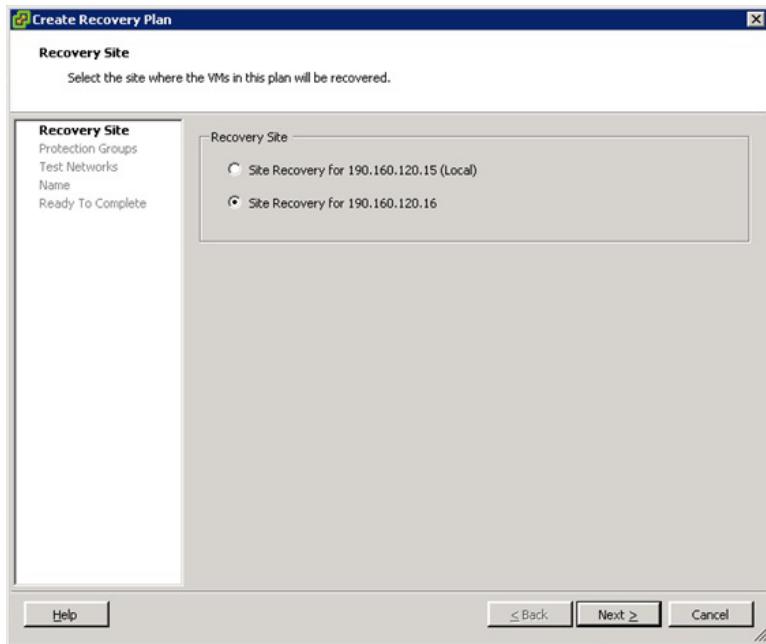


Figure 17. Creating a Recovery Plan

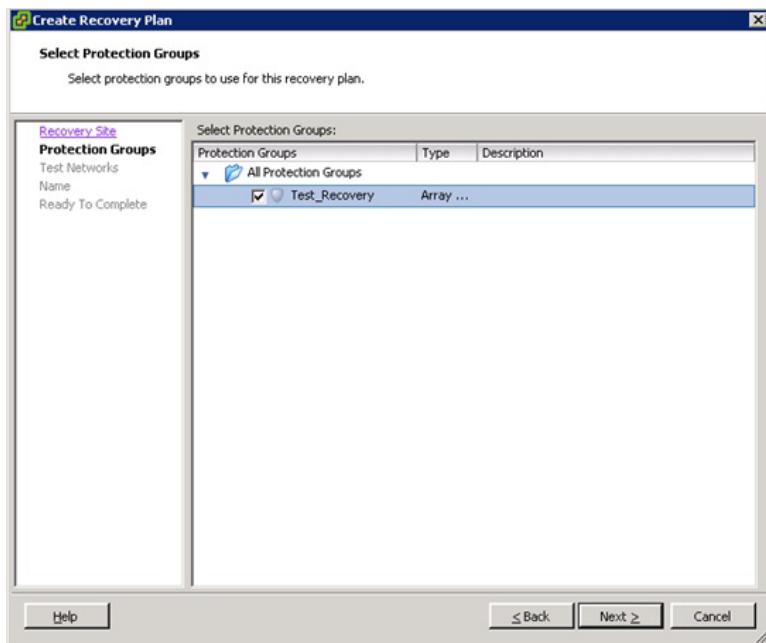
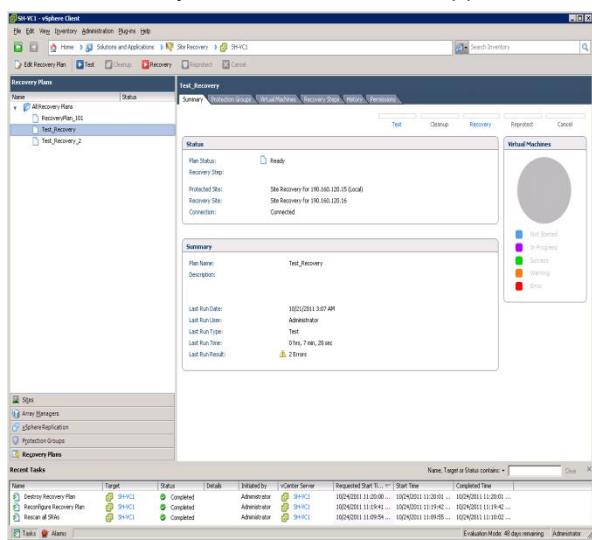


Figure 18. Select Protection Groups

3. In **Select Protection Groups**, select the protection groups for the plan to recover.
4. Click **Next**.
5. In **Test Networks**, select a recovery site network to which virtual machines will connect during recovery plan tests.
6. Click **Next**.
7. Enter name and optional description for the recovery plan and click **Next**.

8. Click **Finish** to create the recovery plan.
9. Click the **Summary** tab and review the recovery plan information shown.



**Figure 19. Recovery Plan Summary**

# Testing And Running Recovery Plans

## Testing Recovery Plans

After creating a recovery plan, test it to verify that it functions as expected.

1. From the **Recovery Plans** view, select the **Summary** tab.
2. Select a recovery plan in the left pane and click **Test**.
3. Choose **Replicate recent changes to recovery site** to ensure that the recovery site has the latest copy of protected virtual machines. Choosing this option will cause synchronization to take longer to complete.
4. Review the confirmation window and click **Finish**.
5. Monitor the recovery plan by selecting the **Recovery Steps** tab.

The recovery plan steps through the process of creating virtual disk snapshots on the storage array, mapping snapshot virtual disks to the ESX host, rescanning to detect new devices, and powering on the VMs.

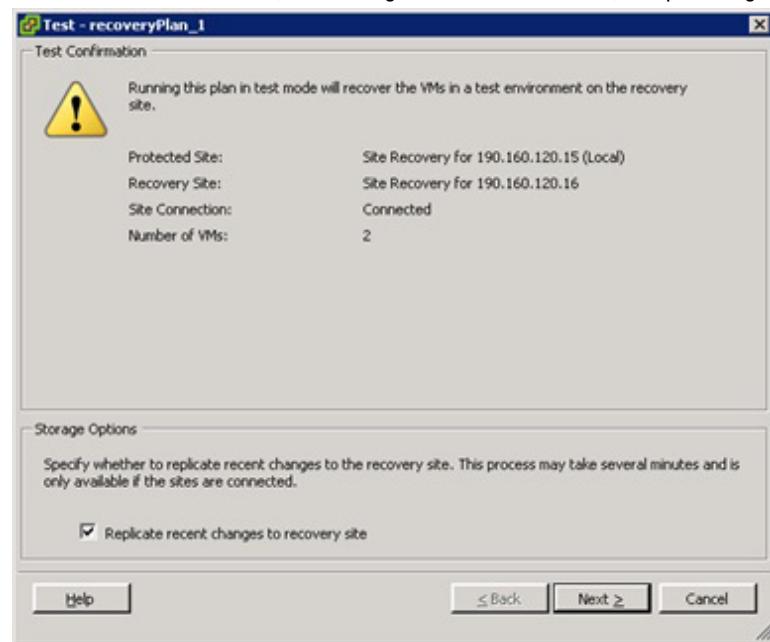
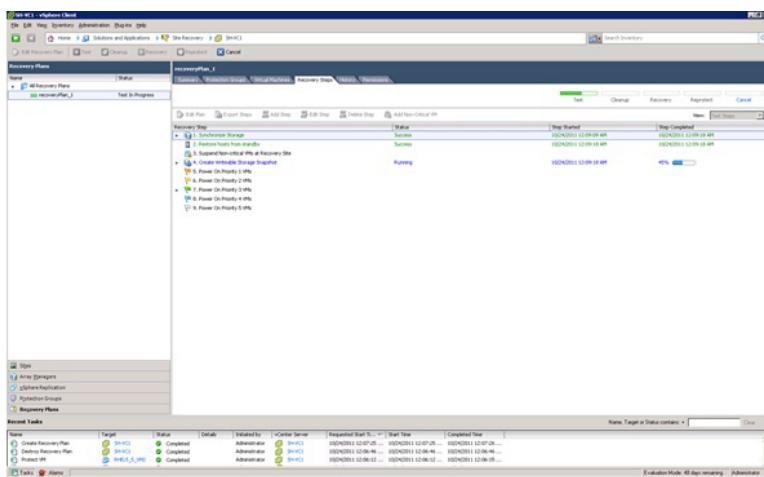


Figure 20. Recovery Plan Summary



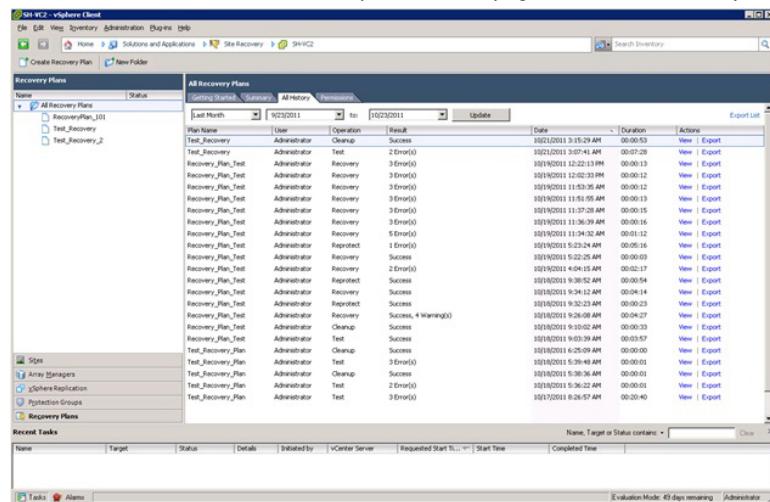
**Figure 21. Recovery Plan Progress**

Once the VMs are powered on and the OS heartbeat has been detected, the test failover plan stops and a yellow continue banner is displayed. To verify the functionality of the failed-over VMs, select the **Host and Clusters** view by typing Ctrl-Shift-H. You will see the VMs powered on under the Recovery Site resource tree. You can open a console to one of the VMs and log in to verify functionality of the guest.

**Note:** Because this is a test failover, network resource configuration has not been applied to the VMs. Therefore, you cannot access any other network resources from these VMs.

Once you are satisfied with the operation of the VMs, return to the Site Recovery view and click on the **Cleanup** link to clean up the test failover. Clicking on this link powers off the test VMs and removes the virtual disk snapshots and returns the recovery plan to the ready state.

After the test failover is complete, click on the **History** tab to see a list of tasks performed on the recovery plan. Click on the **View** link next to the test run to open an HTML page view of the recovery steps performed during the test failover.



**Figure 22. Recovery Plan History View**

## Running Recovery Plans

Running a recovery plan operates similarly to testing a recovery plan. However, it differs in the following ways:

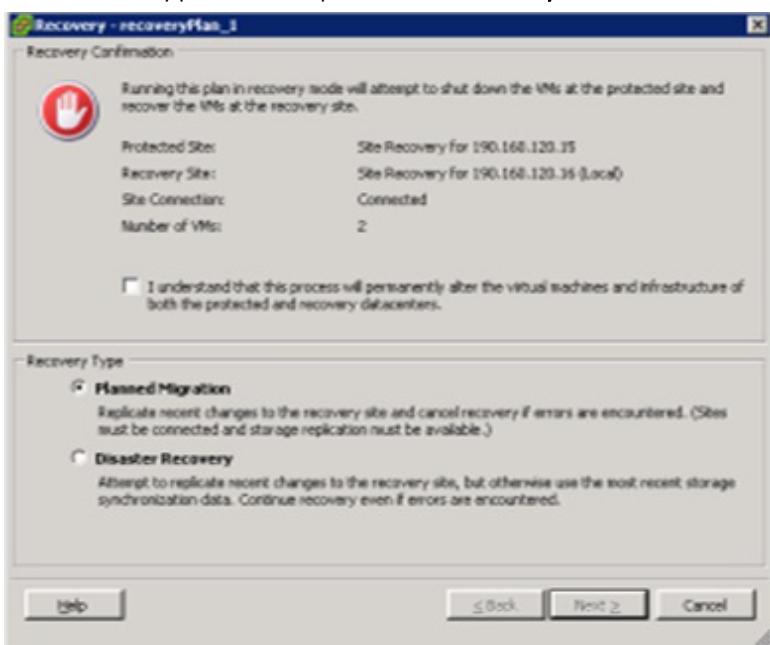
- Remotely replicated virtual disks on the recovery array are promoted to primary status
- Source virtual disks become read-only to the mapped hosts
- Virtual machines on the primary site are powered off
- Network resource configurations are applied to the virtual machines at the recovery site

In the event communication between the recovery site and the protected site is unavailable, the recovery plan is executed and the following occurs:

- The remote replication relationship of the affected virtual disks is broken, requiring a complete resynchronization when communication is re-established
- The virtual machines at the protected site are not powered off and might cause network issues when the network link is re-established

To run a recovery plan

1. From the **Recovery Plans** view, select the **Summary** tab.
2. Select a recovery plan in the left pane and click **Recovery**.



**Figure 23. Run Recovery Plan Warning**

3. In **Recovery Type**, choose either **Planned Migration** or **Disaster Recovery**.

**NOTE:** Choosing the Disaster Recovery option will force a recovery and should be used only when a site has been completely lost. The Planned Migration option will cause recovery to stop if problems are encountered.

4. Review the warning information and select the option acknowledging that you understand the consequences of running the recovery plan. Then, click **Next**.
5. Click **Start** to run the recovery plan.
6. Monitor the recovery plan by selecting the **Recovery Steps** tab.

The **History** tab provides details on the recovery plan process. Once the recovery plan has completed, verify that each of the virtual machines has successfully failed over and is fully operational and that network configuration is established.

# 6

## Fallback Procedures

In order to failback virtual machines from the recovery site to the original protected site, the same procedures for configuring array managers, inventory mappings, and creating recovery plans and protection groups must be performed on the opposite vCenter Server site.

1. If the virtual disk remote replication relationships have been broken, you must recreate the replications from the recovery site storage array to the original protected site storage array, then wait for full synchronization to occur before executing the failback recovery plan.
2. When configuring the array managers, the protected array information now becomes the recovery site storage array information and the recovery array information becomes the original protected site storage array information.
3. Before creating the failback protection groups, you must log into the original protected site vCenter Server and remove the VMs that have been failed over from inventory.
4. The failback recovery plan is created and executed from the original protected site vCenter Server.

Once all these steps have been reversed and the virtual disk remote replication has completed, you can perform the same procedures for Testing Recovery Plans or Running Recovery Plans to restore the virtual machines from the recovery site to the original protected site.

# Troubleshooting and Miscellaneous Issues

This section contains common troubleshooting information and describes miscellaneous issues that might occur during your installation.

## Rescan During Failover Not Detecting Virtual Disk Mappings

Depending on the type of Fibre Channel cards and iSCSI configuration used in the ESX hosts, you might encounter errors during the test failover stating that the datastore volumes cannot be located. If issuing a **rescan all** command from the Storage Adapters view under the Configuration tab for the ESX host does detect the virtual disk mappings, modify the **C:\Program Files (x86)\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml** file to execute two rescans every time the recovery plan is executed by adding **<hostRescanRepeatCnt>2</hostRescanRepeatCnt>** within the **<SanProvider>** section.

```

134
135      <hostRescanTimeoutSec>1200</hostRescanTimeoutSec>
136      <!--
137      Rescan twice for new storage volumes.
138  -->  <hostRescanRepeatCnt>2</hostRescanRepeatCnt>
139      </SanProvider>
140      <!--
141      If this is set to true, when we establish NFC connections (For example to customize
142      the running on an ESX 3.x server), an error in the server's certificate will be
143

```

Figure 24. Repeat Rescan Syntax

## Removing The Snap-XXX- Prefix On Failed-Over Datastores

To restore the name of the datastores to their original name after a failover, modify the **vmware-dr.xml** file by locating **<fixRecoveredDatastoreNames>false</fixRecoveredDatastoreNames>** and by changing false to true.

 **NOTE:** When changing XML configuration files, always remember to save the file before exiting.

```

136      <!-- Stripping off "snap-xxx-" prefix.
137  -->  <fixRecoveredDatastoreNames>true</fixRecoveredDatastoreNames>
138      <!--
139      Timeout in seconds for execution of a single command using array
140      command adapter.
141

```

Figure 25. Fix Datastore Names Syntax

## Debugging SRA Errors

If you encounter an error indicating a problem with the SRA, review the latest **vmware-dr-x.log** file for indications of the error condition. These logs are located under **C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs**. Errors registered from the SRA have an **[#x]** (x denoting a number) at the beginning of the line.

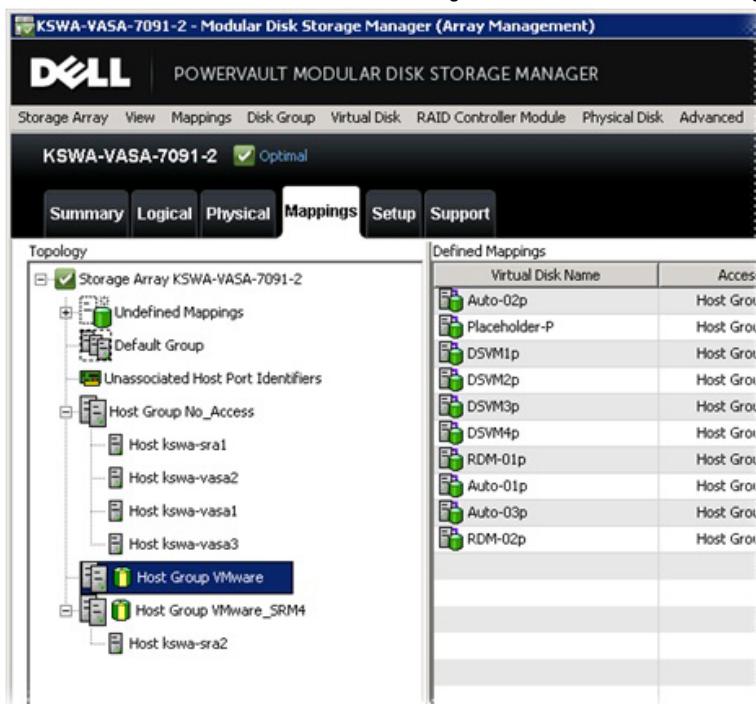
```

2837 [2011-06-30 08:23:26.231] 05864 info "com.vmware.vcDr.San.ArrayManager.AddHrrayTask Task' Work in action threw MethodFault: Dr.san.Fault.InvalidScriptOutput" "N
2838 [2011-06-30 08:23:26.231] 05864 info "com.vmware.vcDr.San.ArrayManager.AddHrrayTask-Task" Fault: "N
2839 [dr.san.Fault.InvalidScriptOutput] ("N
2840 [81] faultCode = "MethodFault";
2841 [81] faultString = "MethodFault null." "N
2842 [81] reason = "Missing LUN identification", "N
2843 [81] msg = "", "N
2844 [81] );" "N
2845 [2011-06-30 08:23:26.231] 05864 verbose "PropertyProvider" RecordOp ASSIGN: Info.error, com.vmware.vcDr.San.ArrayManager.AddHrrayTask-# "N
2846 [2011-06-30 08:23:26.231] 05864 verbose "com.vmware.vcDr.San.ArrayManager.AddHrrayTask-Task" Error set to (dr.san.Fault.InvalidScriptOutput) {"N
2847 [81] faultCode = "MethodFault";
2848 [81] faultString = "MethodFault null." "N
2849 [81] reason = "Missing LUN identification", "N
2850 [81] msg = "", "N
2851 [81] );" "N
2852 [2011-06-30 08:23:26.232] 05864 verbose "PropertyProvider" RecordOp ASSIGN: Info.completeTime, com.vmware.vcDr.San.ArrayManager.AddHrrayTask-# "N
2853 [2011-06-30 08:23:26.232] 05864 verbose "com.vmware.vcDr.San.ArrayManager.AddHrrayTask-Task" State set to error" "N
2854 [2011-06-30 08:23:26.232] 05864 verbose "PropertyProvider" RecordOp ASSIGN: Info.state, com.vmware.vcDr.San.ArrayManager.AddHrrayTask-# "N
2855 [2011-06-30 08:23:26.232] 05864 verbose "PropertyProvider" RecordOp ASSIGN: Info.completeTime, com.vmware.vcDr.San.ArrayManager.AddHrrayTask-# "N

```

**Figure 26. SRM Log File**

This error indicates that a virtual disk is missing a LUN number. Further investigation into MDSM shows the following:



**Figure 27. MDSM Mappings View**

The **Mappings** view shows a defined host group that has virtual disks mapped to it, but no hosts assigned to the host group – this is an invalid SRA configuration. You must either remove the virtual disk mappings from the host group, or assign a host to the host group.

Other errors can be debugged using similar methods. For problems that cannot be resolved, contact Dell support at [dell.com/support](http://dell.com/support) or search for similar issues on the VMware Communities site at <http://communities.vmware.com/index.jspa>.

# Reference Information

## Contacting Dell

-  **NOTE:** If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Go to [dell.com/contactdell](http://dell.com/contactdell).
2. Verify your country or region from the drop-down menu at the top left corner of the page.
3. Select your support category: **Technical Support, Customer Support, Sales, or International Support Services.**
4. Select the appropriate service or support link based on your requirement.

-  **NOTE:** If you have purchased a Dell system, you may be asked for the Service Tag.

## Related Documentation (Other Information You May Need)

-  **NOTE:** For all PowerEdge and PowerVault documentation, go to [dell.com/support/manuals](http://dell.com/support/manuals) and enter the system Service Tag to get your system documentation.
-  **NOTE:** For all Virtualization documents, go to [dell.com/virtualizationsolutions](http://dell.com/virtualizationsolutions).
-  **NOTE:** For all operating system documents, go to [dell.com/operatingsystemmanuals](http://dell.com/operatingsystemmanuals).
-  **NOTE:** For all storage controllers and PCIe SSD documents, go to [dell.com/storagecontrollermanuals](http://dell.com/storagecontrollermanuals).
-  **NOTE:** For Dell Support Forums, go to [en.community.dell.com/support-forums/default.aspx](http://en.community.dell.com/support-forums/default.aspx).
-  **NOTE:** For Dell Advanced Search , go to [search.dell.com/index.aspx](http://search.dell.com/index.aspx).

Your product documentation includes:

<b>Getting Started Guide</b>	Provides an overview of system features, setting up your system, and technical specifications. This document is also shipped with your system.
<b>Owner's Manual</b>	Provides information about system features and describes how to troubleshoot the system and install or replace system components.
<b>Deployment Guide</b>	Provides information about the deployment of the storage controllers, system requirements, storage array organization, and utilities.
<b>Best Practices Guide</b>	Provides information on Installing and Configuring, Asynchronous Remote Replication and Snapshot Repository Sizing.

## VMware Support Information

- vCenter SRM Documentation  
[vmware.com/support/pubs/srm\\_pubs.html](http://vmware.com/support/pubs/srm_pubs.html)
- vSphere Documentation (ESXi, ESX, and vCenter Server)  
[vmware.com/support/pubs/vs\\_pubs.html](http://vmware.com/support/pubs/vs_pubs.html)
- VMware Knowledge Base (Searchable Support Issues)  
[kb.vmware.com/selfservice/microsites/microsite.do](http://kb.vmware.com/selfservice/microsites/microsite.do)
- VMware Communities (Help Forums)  
[communities.vmware.com/index.jspa](http://communities.vmware.com/index.jspa)
- VMware Compatibility Guide  
[vmware.com/resources/compatibility/search.php](http://vmware.com/resources/compatibility/search.php)

## Locating Your System Service Tag

Your system is identified by a unique Express Service Code and Service Tag number. The Express Service Code and Service Tag are found on the front of the system by pulling out the information tag. This information is used by Dell to route support calls to the appropriate personnel.

## Documentation Feedback

If you have feedback for this document, write to [documentation\\_feedback@dell.com](mailto:documentation_feedback@dell.com). Alternatively, you can click on the **Feedback** link in any of the Dell documentation pages, fill out the form, and click **Submit** to send your feedback.