EMC²
where information lives®

VMware Site Recovery Manager with EMC CLARiiON CX3 and MirrorView/S

Implementation Guide

EMC Global Solutions Operations

EMC Corporation
Corporate Headquarters
Hopkinton MA 01748-9103
1.508.435.1000
www.EMC.com

Published July 2008

VMware Site Recovery Manager with EMC CLARiiON CX3 and MirrorView/S Implementation Guide

P/N H5583

Contents

Chapter 2 Installation and Configuration

Chapter 3 Validation

Chapter 4 Recommendations and Conclusion

About this Document

Purpose

EMC solution architects were given access to an EMC lab environment to install, configure, validate the operation of, and document a disaster recovery plan using VMware Site Recovery Manager (SRM) for ESX Server 3.5 virtual machines with EMC CLARiiON CX3 storage systems. This guide provides an illustrated walkthrough of this exercise, with example screenshots and command line input, for individuals attempting to implement such a solution in the field.

Audience

This guide is intended for system engineers attempting to implement a disaster recovery solution using VMware Site Recovery Manager (SRM) for ESX Server 3.5 virtual machines with CLARiiON CX3 storage systems.

It is assumed that the reader is already familiar with ESX Server 3.5 virtual machines, EMC CLARiiON storage systems, EMC MirrorView/S and SnapView software, and VMware Site Recovery Manager (SRM) software.

Scope

This guide attempts to bridge a potential information gap between the administration guide for VMware Site Recovery Manager and the release notes for EMC MirrorView Storage Replication Adapter for VMware Site Recovery Manager (see "Scope of EMC MirrorView Storage Replication Adapter for SRM release notes" and "Scope of VMware Site Recovery Manager administration guide" on page 6).

This guide does not reproduce the information in the previously mentioned documents. Instead, it provides an illustrated walkthrough, with example screenshots and command line input, of the processes of setting up and testing a disaster recovery plan using SRM for ESX Server 3.5 virtual machines with EMC CLARiiON storage systems. Also included are a limited set of recommendations for individuals attempting to implement such a solution in the field.

Scope of EMC MirrorView Storage Replication Adapter for SRM release notes

The EMC MirrorView Storage Replication Adapter for SRM release notes provide information about installing and configuring the Storage Replication Adapter (SRA) for EMC CLARiiON systems. The release notes include:

- Environment and system requirements, including CLARiiON storage system requirements
- Known problems and limitations
- Instructions for configuring storage system LUNs to protect a virtual machine, an explanation of MirrorView consistency groups and SRM protection groups, and instructions for connecting to and configuring storage systems
- Prerequisites and instructions for installing the EMC MirrorView Storage Replication Adapter for SRM plug-in on both the protected and recovery SRM servers

Scope of VMware Site Recovery Manager administration guide

The VMware Site Recovery Manager administration guide provides information about installing and configuring SRM, including conceptual overviews of configuring and managing protection sites, recovery planning, testing, and performing failover, alerts, system management, and troubleshooting.

Related documents

The following documents provide additional, relevant information.

- *EMC MirrorView Adapter for VMware Site Recovery Manager Release Notes* (EMC Powerlink)
- *Administration Guide for Site Recovery Manager* (http://www.VMware.com)
- *White Paper: CLARiiON SnapView Snapshots and Snap Sessions Knowledgebook—A Detailed Review* (EMC Powerlink)
- *White paper: MirrorView Knowledgebook: FLARE 26 - Applied Technology* (EMC Powerlink)

1 Implementation Overview

This chapter includes the following topics:

Introduction

The increasing demand for server consolidation to contain hardware and data center environment costs has accelerated the deployment of server virtualization technology into the data center. Customers are deploying VMware ESX Server into ever-increasing parts of their infrastructures, in many cases as a first choice for server platform deployment for tier-1 and tier-2 applications. As more business-critical applications are deployed as virtual servers, it is important to integrate VMware into the business continuity planning process. To facilitate recovery of virtual server environments, VMware has introduced Site Recovery Manager, an integrated disaster recovery workflow application that automates and controls the site-to-site failover of virtual machines in the event of a disaster.

Site Recovery Manager (SRM) is an integral component of the VMware infrastructure that is installed within a VirtualCenter controlled VMware data center. SRM leverages the data replication capability of the underlying storage array to create a workflow that will fail over selected virtual machines from a "protected site" to a "recovery site" and bring the virtual machines and their associated applications back into production at the recovery site. SRM accomplishes this by communicating with and controlling the underlying storage replication software through an SRM plug-in, known as a Storage Replication Adapter (SRA). EMC has written, tested, and released SRAs for its storage replication products.

SRM is installed into a new or existing ESX Server environment that has intelligent array storage. Through SRM, the administrator defines virtual machines at the protected site that are to be incorporated into a "recovery plan." Virtual machines in a recovery plan must have data stores on an array that is replicating the underlying devices supporting the data store. The recovery plan defines the actions that are to be taken for a selected set of virtual machines in the event of an administrator-initiated failover from the protected site to the recovery site. The recovery plan will shut down virtual machines at the protected site, prepare storage for device/LUN recovery and use at the recovery site, and initiate startup of virtual machines at the recovery site.

Component overview

The basic components of a disaster recovery solution using VMware Site Recovery Manager with EMC® CLARiiON® CX3 storage are described in this section.

VMware Site Recovery Manager

VMware Site Recovery Manager (SRM) is a disaster recovery framework that integrates with various EMC replication software products (for example, MirrorView™/S for CLARiiON) to automate the failover process of virtual machines. SRM recovery plans leverage the array-based snapshot features to test the failover process to ensure that the secondary image is consistent and usable. SRM relies on two independent VMware VirtualCenter servers to be in place at both the protected (primary) site and at the recovery (secondary) site to facilitate the failover process between the two sites. Array-based Storage Replication Adapters (SRAs) are also installed at both sites in order to talk to the storage-systems independently (see Storage Replication Adapter below).

EMC MirrorView/S

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

Storage Replication Adapter

A Storage Replication Adapter (SRA) is software provided by storage vendors that ensures integration of storage devices and replication with VMware Site Recovery Manager. These vendor-specific scripts support array discovery, replicated LUN discovery, test failover, and actual failover. The EMC MirrorView Storage Replication Adapter for VMware Site Recovery Manager is a software package that allows SRM to implement disaster recovery for ESX Server 3.5 virtual machines using CLARiiON CX3 storage systems running MirrorView/S and SnapView™ software. MirrorView/S over both iSCSI and Fibre Channel direct and SAN connections are supported.

Logical architecture

Figure 1 illustrates the overall logical architecture of the integration scenario.

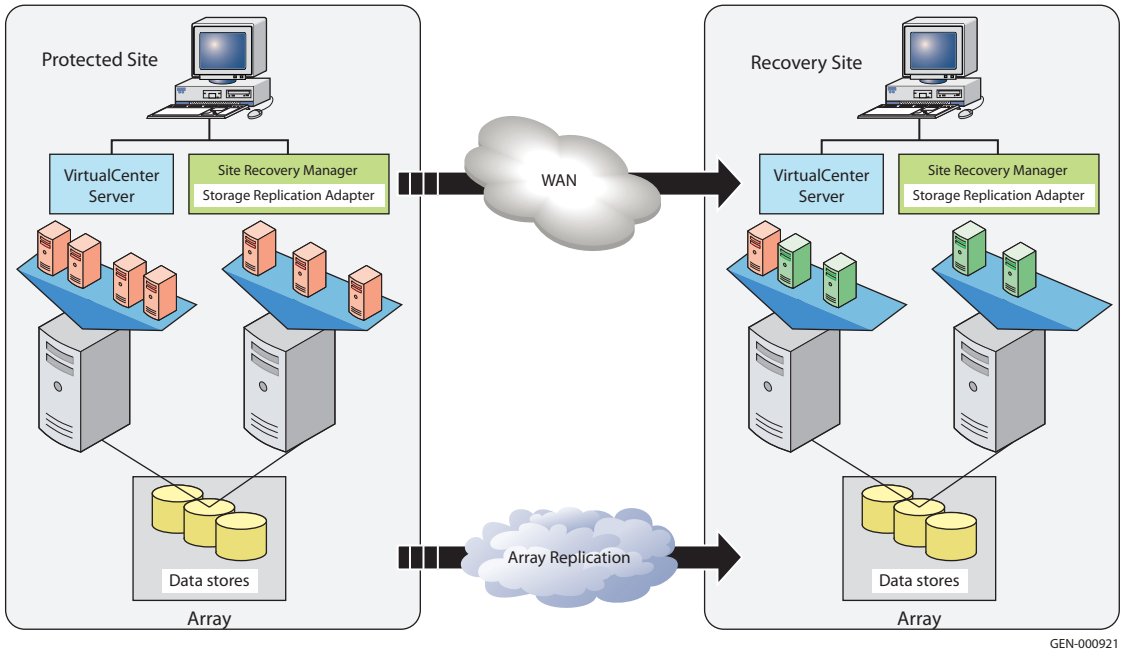


Figure 1 Overall logical architecture

Hardware and software resources

Table 1 and Table 2 present the hardware and software used in this specific implementation scenario

Table 1 Hardware resources

Equipment	Quantity	Configuration
Storage arrays	2	EMC CLARiiON CX3 running FLARE® version 03.26 with MirrorView/S and SnapView enablers
Commodity servers	4	Dell PowerEdge 2950 Windows hosts configured as VMware VirtualCenter servers running VMware ESX Server 3.5
Network switch	1	Cisco 4506
Fibre Channel switch	1	Cisco MDS 9513

Table 2 Software resources

Software title	Version	Purpose
VMware ESX Server	3.5	Installed on VMware VirtualCenter servers
VMware Site Recovery Manager	1.0	Installed on VMware VirtualCenter servers
EMC Solutions Enabler	6.5	Installed on VMware VirtualCenter servers
.NET Framework	2.0	Installed as part of VMware VirtualCenter
EMC MirrorView SRA for SRM	1.0	Installed on VMware VirtualCenter servers
EMC Navisphere® Manager	3.26.020.5.014	Can be installed on any network client
EMC NaviCLI	3.26.020.5.014	Can be installed on any network client
EMC MirrorView/S	3.26.020.5.014	Can be installed on any network client
EMC SnapView	3.26.020.5.014	Can be installed on any network client
EMC Navisphere Service Taskbar	3.26.020.5.014	Can be installed on any network client

2 Installation and Configuration

This chapter includes the following topics:

Introduction

The installation and configuration instructions presented in this section apply to the specific revision levels of components used during the testing of this integration scenario. Before attempting a real-world implementation based on this scenario, gather the appropriate installation and configuration documentation for the revision levels of the hardware and software components that you are planning to include in the implementation. Version-specific release notes are especially important.

See also For environment and system requirements, including EMC CLARiiON storage system requirements, refer to the most recent version of the *EMC MirrorView Adapter for VMware Site Recovery Manager Release Notes*.

Installation and configuration of the various components must be performed in the appropriate sequence and at the appropriate site or sites (protected site, recovery site, or both). Table 3 summarizes the sequence and indicates the site or sites at which each step in the sequence is performed.

Table 3 Installation and configuration process overview

	Action at protected (primary) site	Action at recovery (secondary) site
Initial requirements	VMware ESX Server cluster at protected site VMware VirtualCenter 2.5u1 installed Array with remote replication capability	VMware ESX Server cluster at recovery site VMware VirtualCenter 2.5u1 installed Array with remote replication capability
Step 1	Map virtual machines to be protected to associated storage LUNs	
Step 2		Verify available LUNs to act as a target for array replication
Step 3	Using storage replication management tools, configure target array LUN replication from protected site to recovery site	
Step 4		Verify replication
Step 5	Install VMware Site Recovery Manager (SRM) and EMC Site Recovery Adapter on VirtualCenter server	
Step 6		Install VMware Site Recovery Manager (SRM) and EMC Site Recovery Adapter on VirtualCenter server
Step 7	Using VirtualCenter client, log in to VirtualCenter server at protected site and configure connection to VirtualCenter server	

Table 3 Installation and configuration process overview (continued)

	Action at protected (primary) site	Action at recovery (secondary) site
Step 8		Using VirtualCenter client, log in to VirtualCenter server and configure connection to accept pairing with protected site
Step 9	Using VirtualCenter client, log in to VirtualCenter server and configure array managers, inventory mappings, and protection groups	
Step 10		Using VirtualCenter client, log in to VirtualCenter server and create recovery plan
Step 11		Test/execute recovery plan

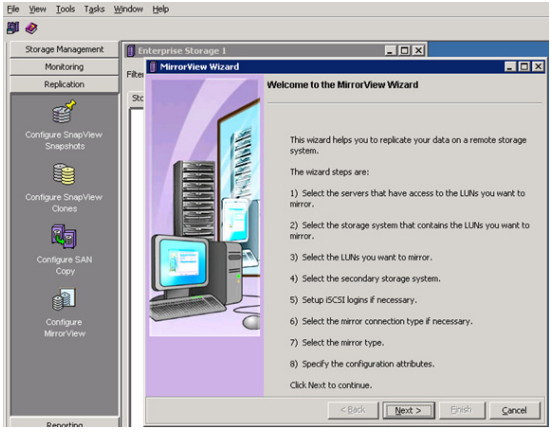
Configuring MirrorView/S for Site Recovery Manager

To configure MirrorView/S for Site Recovery Manager, you can use either

- Navisphere Manager Configure MirrorView Wizard,
- NaviCLI, or
- Navisphere GUI

This section shows how to use the wizard and CLI, but not the GUI.

To use the Navisphere Manager Configure MirrorView Wizard, launch the wizard and follow the step-by-step instructions it presents.



Note: MirrorView SRA supports only the MirrorView/S mirror type. Selecting a sync rate of High is recommended.

To use NaviCLI:

1. Identify the LUNs to be protected with SRM.
2. Create paths for remote mirroring between the protected and recovery CLARiiON.

```
naviseccli -h SP ipaddress mirror -sync -enablepath SPhostname
   [-connection type fibre|iscsi]
```

3. Create remote mirrors of the LUNs. The LUNs on which the mirrors are created become the primary images.

```
naviseccli -h SP ipaddress mirror -sync -create -lun <LUN_Number>
```

4. On the remote CLARiiON, add the secondary images to the primary images and start the initial synchronization between the protected and secondary images. The following command assumes that the LUNs are already created on the remote CLARiiON.

```
naviseccli -h SP ipaddress mirror -sync -addimage -name <name> -arrayhost
   <sp-hostname| sp ipaddress> -lun <lunnumber| lun uid>
```

5. Even if there is only a single LUN being replicated to the recovery site, you must create a consistency group for SRM. The following commands show how to create a consistency group and add existing mirrors to the consistency group.

```
naviseccli -h SP ipaddress mirror -sync -creategroup -name <name>
naviseccli -h SP ipaddress mirror -sync -addgroup -name <name> -mirrorname
   <mirrorname>
```

6. If the mirrors are fractured, the syncimage option can be used to resynchronize the protected and secondary images:

```
naviseccli -h SP ipaddress mirror -sync -syncgroup -name <name>
```

7. While the mirrors are synchronizing or once they arrive at a consistent state, you can add all the LUNs (if you have not already done so) to the ESX Server CLARiiON Storage Group at the protected and recovery sites using the following command:

```
naviseccli -h SP ipaddress storagegroup -addhlu -gname <ESX CLARiiON
   Storage Group Name> -hlu <Host Device ID> -alu <Array LUN ID>
```

Configuring SnapView snapshots

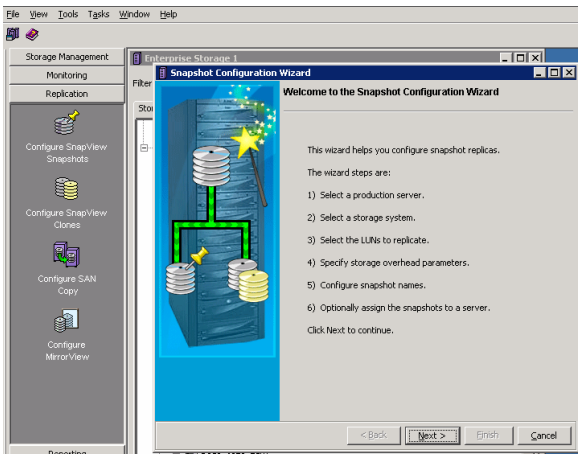
Note: Configure snapshots on the VirtualCenter client connected to the protected site and also the VirtualCenter client connected to the recovery site.

To configure SnapView snapshots you can use either

- Navisphere Manager Configure MirrorView Wizard,
- NaviCLI, or
- Navisphere GUI

This section shows how to use the wizard and CLI, but not the GUI.

To use the Navisphere Manager Snapshot Configuration Wizard, launch the wizard and follow the step-by-step instructions it presents.



The wizard will create LUNs automatically to be placed within the Reserved LUN Pool. The default is to allocate 30% storage capacity to the LUN where the snapshot is created. If this will not be enough capacity for your environment, override the value and select a more appropriate percentage. Using the wizard, add the snapshots to the appropriate CLARiiON storage group at the SRM recovery site.

Important: The SRA requires the string shown in bold to exist somewhere in the snapshot name: **VMWARE_SRM_SNAP**_LUNID

To use NaviCLI:

1. Add the LUNs to be used by SnapView sessions to the reserved LUN pool.

   ```
   naviseccli -h SP ipaddress reserved -lunpool -addlun <LUN
      IDS separated by spaces>
   ```

2. Create a snapshot for each LUN at the recovery site and add the snapshot to the ESX server CLARiiON storage group at the recovery site. This snapshot will not be activated until a user tests the SRM failover operation, during which SRM will start a session and activate it with the corresponding snapshot.

   Important: The SRA requires the string shown in bold to exist somewhere in the snapshot name.

```
naviseccli -h SP ipaddress snapview -createsnapshot <LUN ID> -snapshotname
   VMWARE_SRM_SNAP_LUNID

naviseccli -h SP ipaddress storagegroup -addsnapshot -gname <ESX CLARiiON
   Storage Group name> -snapshotname <name of snapshot>
```

See also For more information on using Navisphere CLI with MirrorView, refer to the *MirrorView/Synchronous Command Line Interface Reference*, available on EMC Powerlink®.

Installing VMware Site Recovery Manager

After configuring SnapView snapshots, the next step is to install the SRM framework, the SRM plug-in, and the MirrorView Storage Replication Adapter for SRM.

See also For more information, including system requirements, refer to the *Administration Guide for Site Recovery Manager* and the *EMC MirrorView Adapter for VMware Site Recovery Manager Release Notes*.

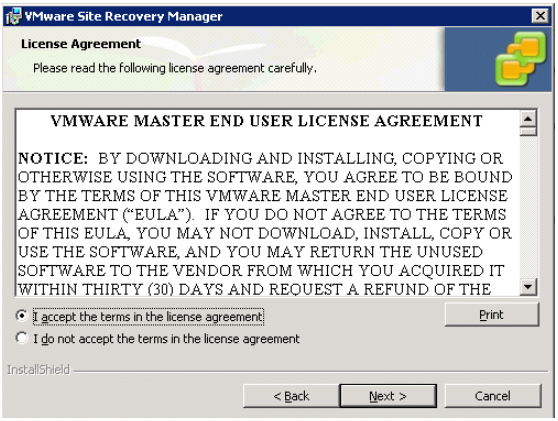
Prerequisites

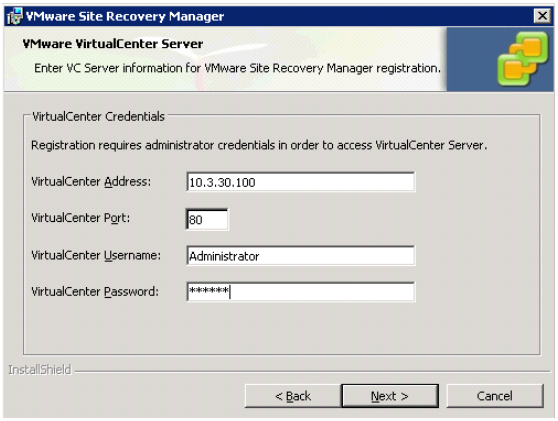
Before you install SRM, MirrorView mirror states must be synchronized or consistent and be part of a consistency group.

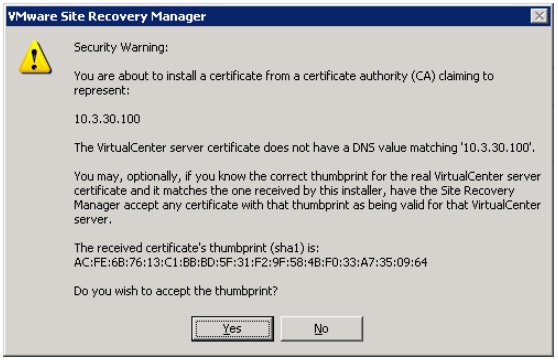
Installing the SRM framework

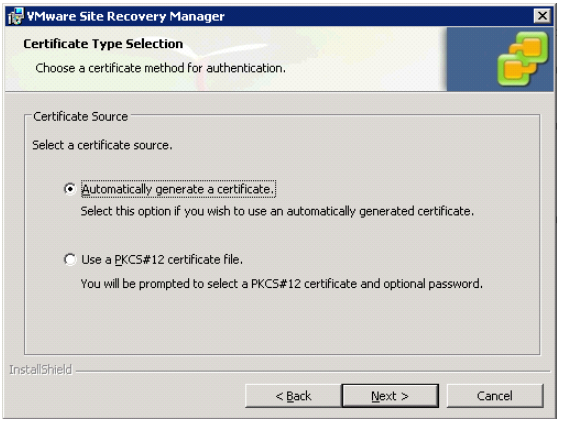
Click on the VMware Site Recovery Manager executable to install the SRM framework and navigate through the installation wizard as shown in the example below (the example sequence flows from left to right, top to bottom).

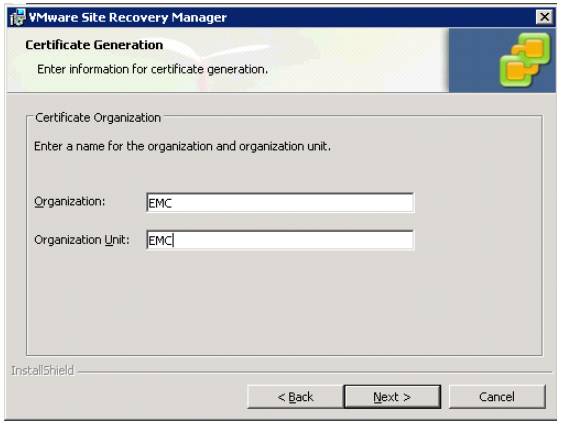
Note: Install this component on the VirtualCenter client connected to the protected site and also the VirtualCenter client connected to the recovery site.

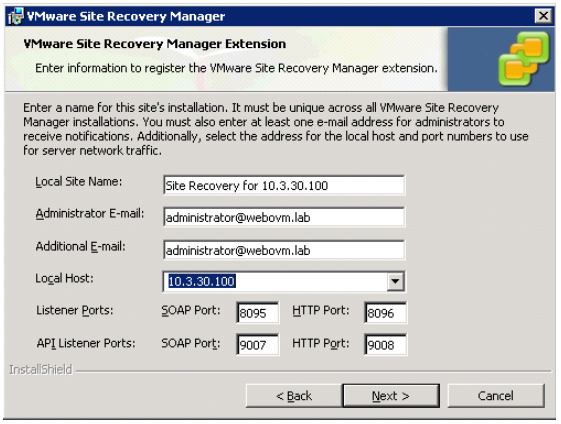


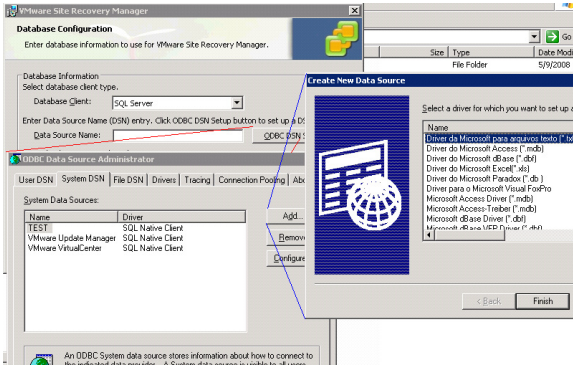


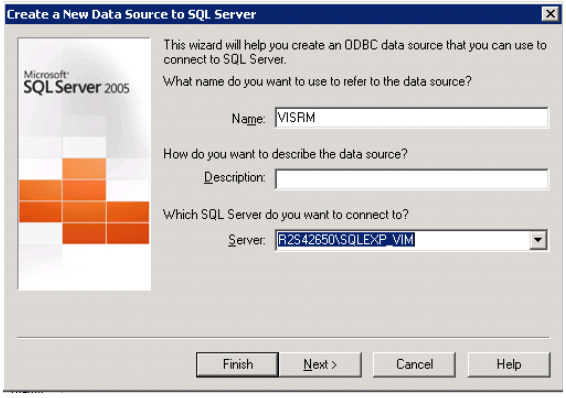


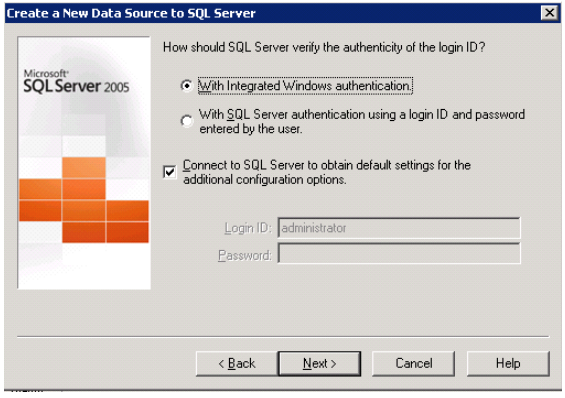

VMware Site Recovery Manager
Certificate Type Selection
Choose a certificate method for authentication.
Certificate Source
Select a certificate source.
Automatically generate a certificate.
Select this option if you wish to use an automatically generated certificate.
Use a PKCS#12 certificate file.
You will be prompted to select a PKCS#12 certificate and optional password.
InstallShield
< Back
Next >
Cancel

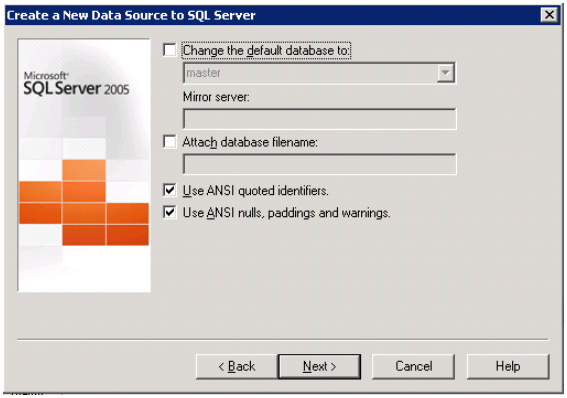

VMware Site Recovery Manager
Certificate Generation
Enter information for certificate generation.
Certificate Organization
Enter a name for the organization and organization unit.
Organization:
EMC
Organization Unit:
EMC
InstallShield
< Back
Next >
Cancel

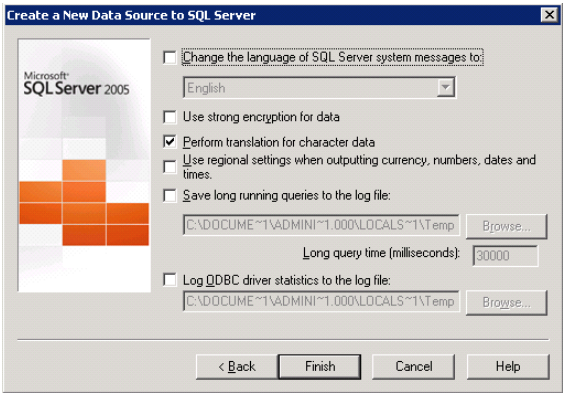

VMware Site Recovery Manager
VMware Site Recovery Manager Extension
Enter information to register the VMware Site Recovery Manager extension.
Enter a name for this site's installation. It must be unique across all VMware Site Recovery Manager installations. You must also enter at least one e-mail address for administrators to receive notifications. Additionally, select the address for the local host and port numbers to use for server network traffic.
Local Site Name:
Site Recovery for 10.3.30.100
Administrator E-mail:
administrator@webovm.lab
Additional E-mail:
administrator@webovm.lab
Local Host:
10.3.30.100
Listener Ports:
SOAP Port:
8095
HTTP Port:
8096
API Listener Ports:
SOAP Port:
9007
HTTP Port:
9008
InstallShield
< Back
Next >
Cancel

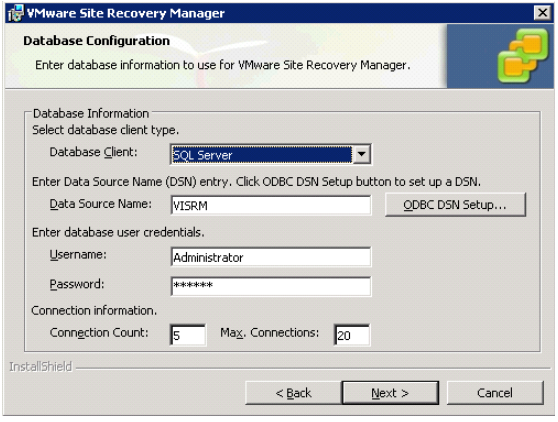

VMware Site Recovery Manager
Database Configuration
Enter database information to use for VMware Site Recovery Manager.
Database Information
Select database client type.
Database Client:
SQL Server
Enter Data Source Name (DSN) entry. Click ODBC DSN Setup button to set up a DSN.
Data Source Name:
ODBC DSN Setup...
ODBC Data Source Administrator
User DSN
System DSN
File DSN
Drivers
Tracing
Connection Pooling
About
System Data Sources:
Name
Driver
TEST
SQL Native Client
VMware Update Manager
SQL Native Client
VMware VirtualCenter
SQL Native Client
Add...
Remove
Configure...
An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users
Create New Data Source
Select a driver for which you want to set up a data source.
Name
Driver do Microsoft para arquivos texto (*.txt;*.csv)
Driver do Microsoft Access (*.mdb)
Driver do Microsoft dBase (*.dbf)
Driver do Microsoft Excel(*.xls)
Driver do Microsoft Paradox (*.db)
Driver para o Microsoft Visual FoxPro
Microsoft Access Driver (*.mdb)
Microsoft Access-Treiber (*.mdb)
Microsoft dBase Driver (*.dbf)
< Back
Finish

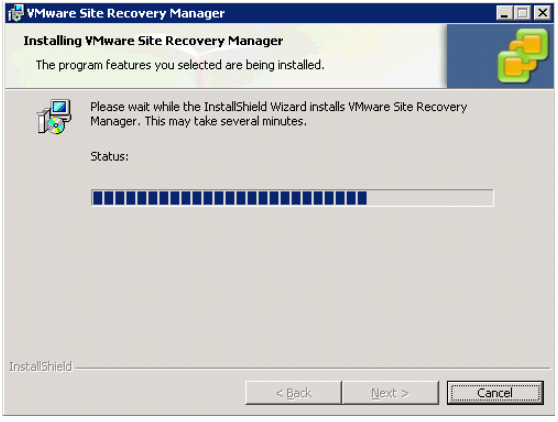

Create a New Data Source to SQL Server
Microsoft SQL Server 2005
This wizard will help you create an ODBC data source that you can use to connect to SQL Server.
What name do you want to use to refer to the data source?
Name:
VISRM
How do you want to describe the data source?
Description:
Which SQL Server do you want to connect to?
Server:
R2S42650\SQLEXP_VIM
Finish
Next >
Cancel
Help


Create a New Data Source to SQL Server
Microsoft SQL Server 2005
How should SQL Server verify the authenticity of the login ID?
With Integrated Windows authentication.
With SQL Server authentication using a login ID and password entered by the user.
Connect to SQL Server to obtain default settings for the additional configuration options.
Login ID:
administrator
Password:
< Back
Next >
Cancel
Help


Create a New Data Source to SQL Server
Microsoft SQL Server 2005
Change the default database to:
master
Mirror server:
Attach database filename:
Use ANSI quoted identifiers.
Use ANSI nulls, paddings and warnings.
< Back
Next >
Cancel
Help


Create a New Data Source to SQL Server
Microsoft SQL Server 2005
Change the language of SQL Server system messages to:
English
Use strong encryption for data
Perform translation for character data
Use regional settings when outputting currency, numbers, dates and times.
Save long running queries to the log file:
C:\DOCUME~1\ADMINI~1.000\LOCALS~1\Temp
Browse...
Long query time (milliseconds):
30000
Log ODBC driver statistics to the log file:
C:\DOCUME~1\ADMINI~1.000\LOCALS~1\Temp
Browse...
< Back
Finish
Cancel
Help

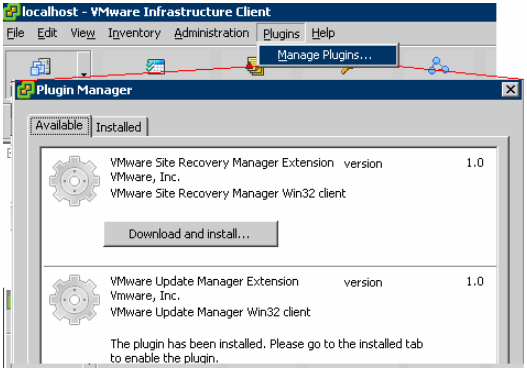

VMware Site Recovery Manager
Database Configuration
Enter database information to use for VMware Site Recovery Manager.
Database Information
Select database client type.
Database Client:
SQL Server
Enter Data Source Name (DSN) entry. Click ODBC DSN Setup button to set up a DSN.
Data Source Name:
VISRM
ODBC DSN Setup...
Enter database user credentials.
Username:
Administrator
Password:
******
Connection information.
Connection Count:
5
Max. Connections:
20
InstallShield
< Back
Next >
Cancel

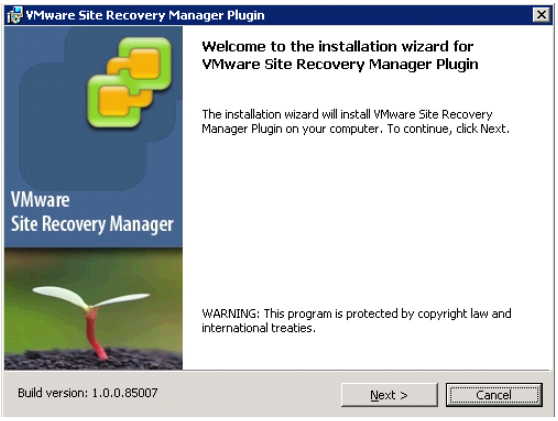

VMware Site Recovery Manager
Installing VMware Site Recovery Manager
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs VMware Site Recovery Manager. This may take several minutes.
Status:
InstallShield
< Back
Next >
Cancel

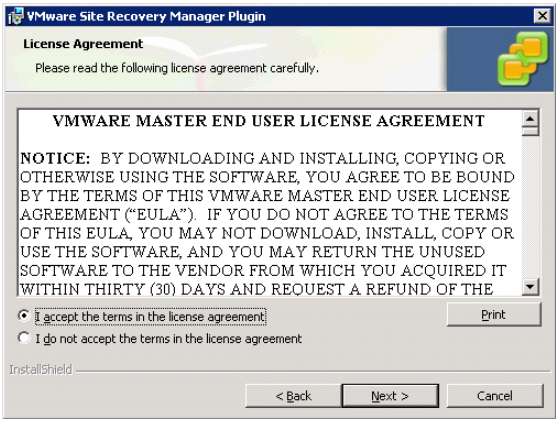
Installing the SRM plug-in

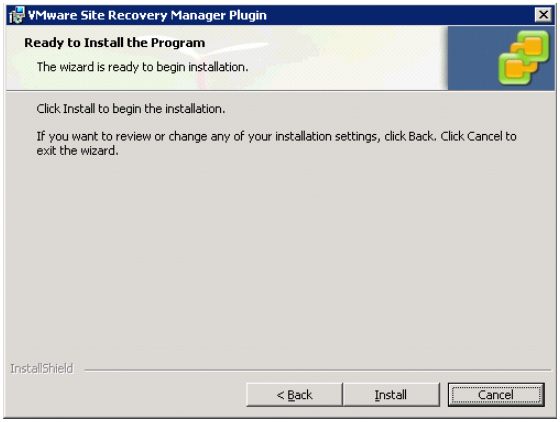
After installing the SRM framework, navigate to Manage Plugins and download and install the SRM plug-in as shown in the example below (the example sequence flows from left to right, top to bottom).

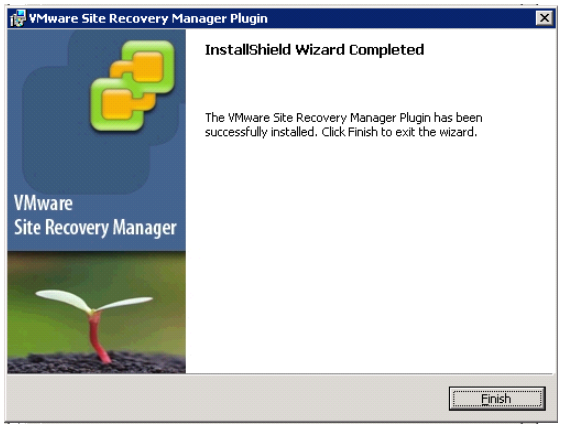
Note: Install this component on the VirtualCenter client connected to the protected site and also the VirtualCenter client connected to the recovery site.

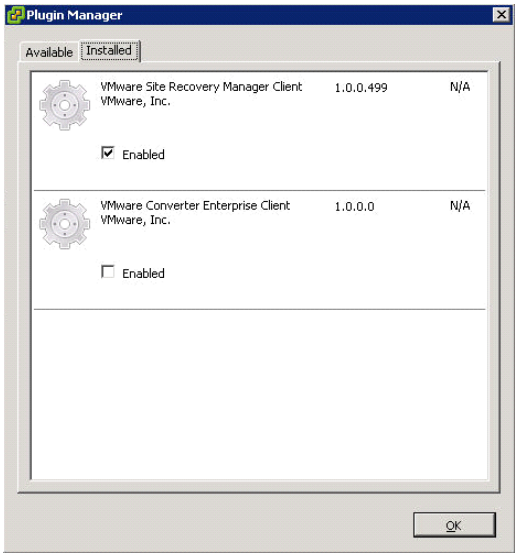












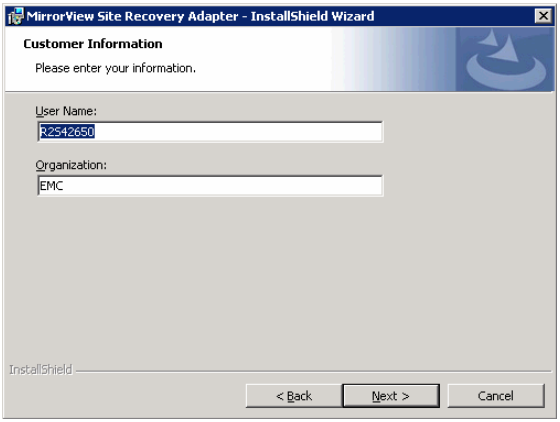
Installing the MirrorView SRA for Site Recovery Manager

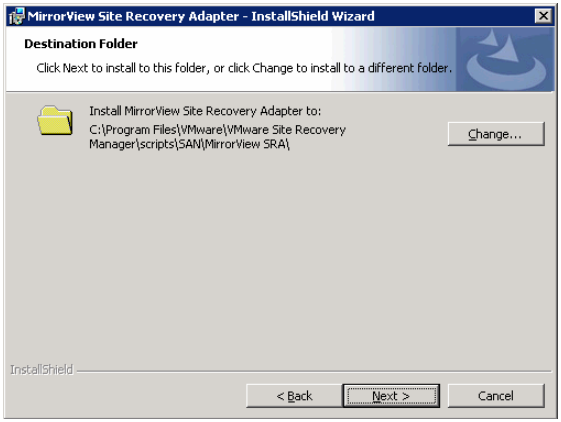
After installing the SRM plug-in, launch the MirrorView Storage Replication Adapter installation wizard and follow the instructions it presents.

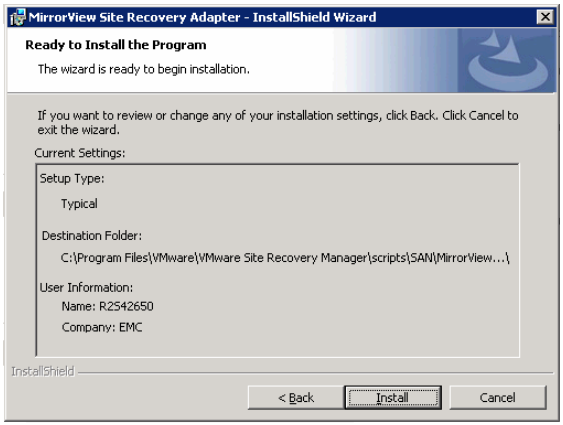
Note: Install this component on the VirtualCenter client connected to the protected site and also the VirtualCenter client connected to the recovery site.

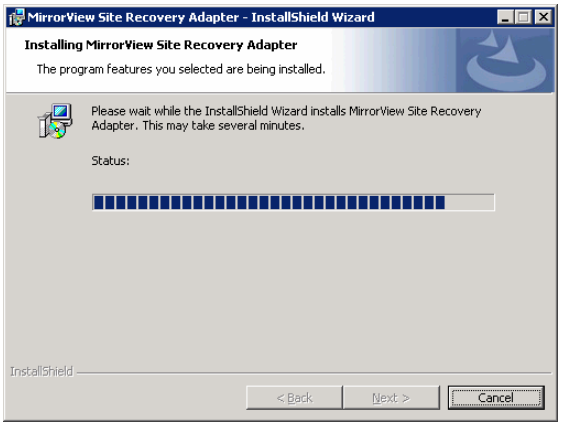

MirrorView Site Recovery Adapter - InstallShield Wizard
Welcome to the InstallShield Wizard for MirrorView Site Recovery Adapter
The InstallShield(R) Wizard will install MirrorView Site Recovery Adapter on your computer. To continue, click Next.
Build 1.0.0.6
< Back
Next >
Cancel

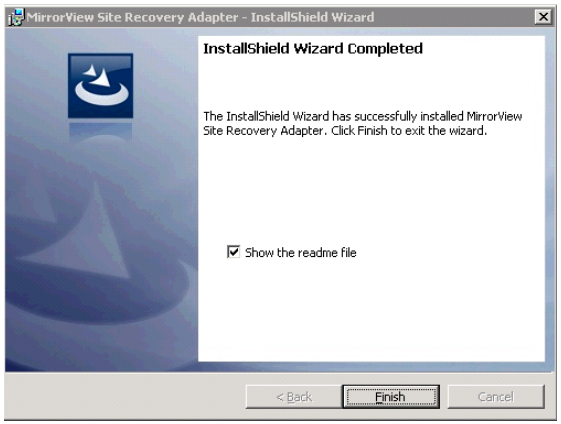

MirrorView Site Recovery Adapter - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Storage Adapter Software License Agreement
IMPORTANT - PLEASE READ CAREFULLY
This Storage Adapter Software License Agreement (the "Agreement") is a legal agreement between EMC Corporation and you (the "Customer"). This agreement governs the Customer's access to,
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel


MirrorView Site Recovery Adapter - InstallShield Wizard
Customer Information
Please enter your information.
User Name:
R2S42650
Organization:
EMC
InstallShield
< Back
Next >
Cancel


MirrorView Site Recovery Adapter - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install MirrorView Site Recovery Adapter to:
C:\Program Files\VMware\VMware Site Recovery Manager\scripts\SAN\MirrorView SRA\
Change...
InstallShield
< Back
Next >
Cancel







Configuring VMware Site Recovery Manager

After installing the MirrorView Storage Replication Adapter for SRM, configure SRM within the environment as follows.

Establishing the connection between sites

Note: Establish the inter-site connection on the VirtualCenter client connected to the protected site and also the VirtualCenter client connected to the recovery site.

1. Log in to the VirtualCenter client.
2. On the toolbar, click the Site Recovery button.

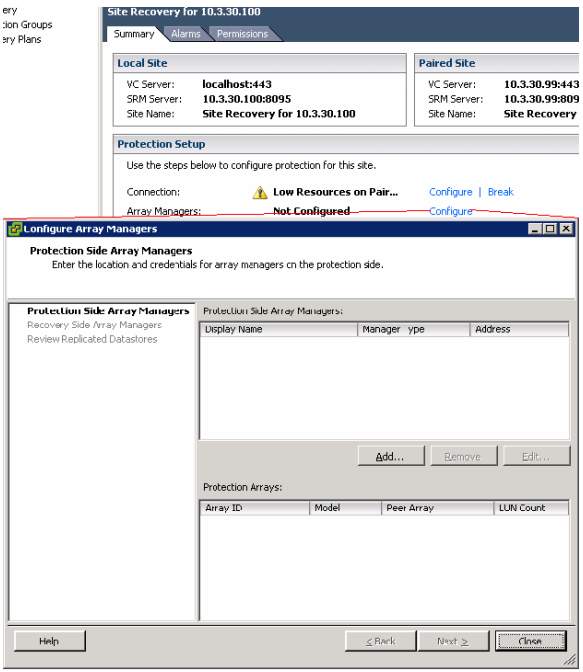
3. Near the center of the Site Recovery screen, notice that the Paired Site field is blank. Under Protection Setup, next to the Connection label, click Configure and add the IP address of the VirtualCenter client at the recovery site to establish a connection.

Configuring array managers

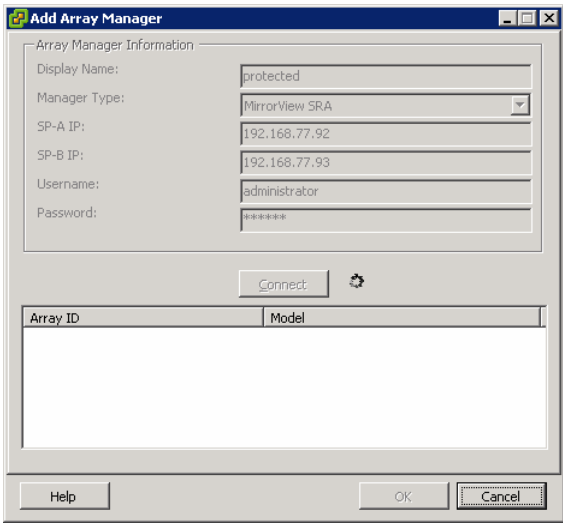
After establishing a connection between the protected and recovery sites, configure array managers as shown in the example below.

Note: Configure array managers on the VirtualCenter client connected to the protected site and also the VirtualCenter client connected to the recovery site.

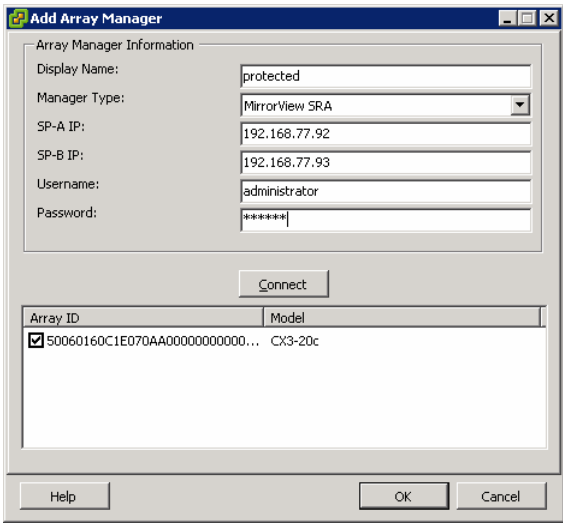
1. From the VirtualCenter client connected to the protected site, under Protection Setup next to the Array Managers label, click Configure.
2. On the Configure Array Managers screen, click the Add button.



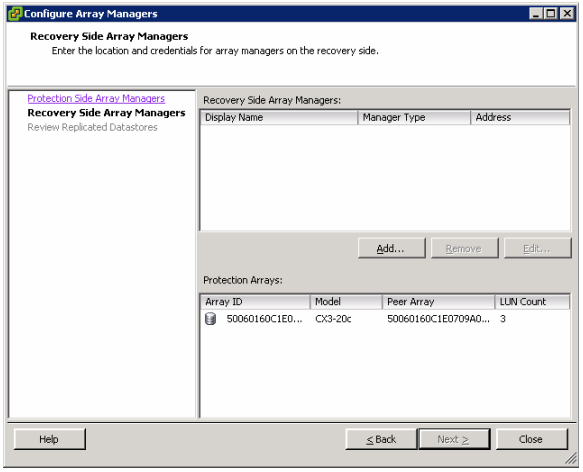
3. On the Add Array Manager screen, specify the array information for the protected site, and click Connect to discover and display the array.

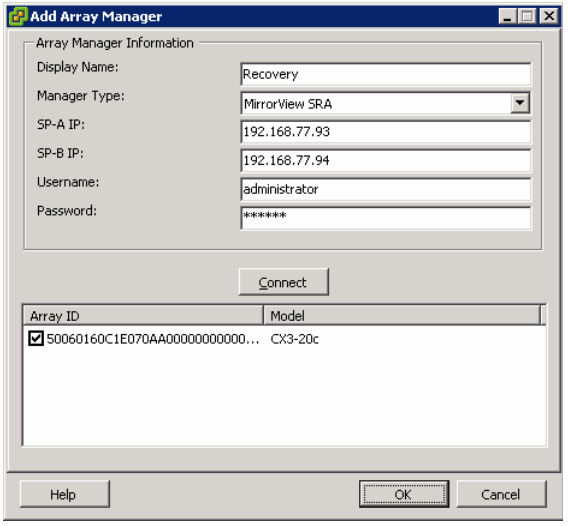


4. Click OK to dismiss the Add Array Manager screen.

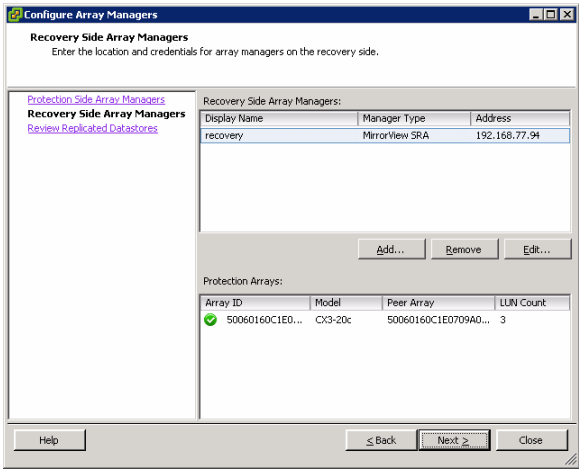


5. Repeat the two previous steps, this time adding an array manager for the recovery site.





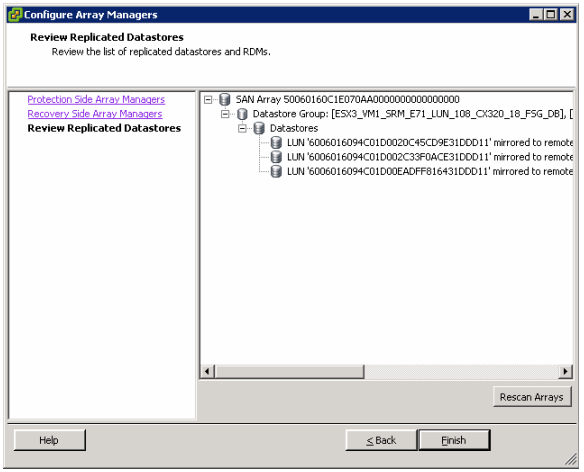
6. Click Next to display all the data stores that are being replicated from the protected site to the recovery site.



7. If you do not see the expected data stores, click Rescan Arrays.

Note: During testing, it was necessary to remove the data stores from the virtual machine and then re-add them in order for SRM to list the virtual disks as replicated.

8. Click Finish. The arrays are now managed.

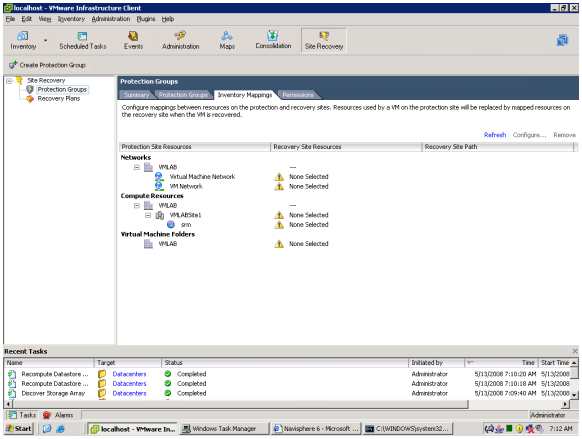


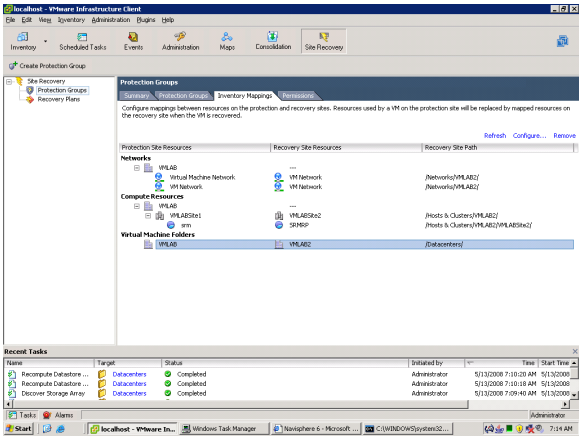
Configuring inventory mappings

After configuring array managers, configure inventory mappings. This involves mapping resources from the protected site to the recovery site.

Note: Configure inventory mapping on the VirtualCenter client connected to the protected site and also the VirtualCenter client connected to the recovery site.

1. In the main window of the VirtualCenter client, click the item that you want to configure. The Configure link in the upper right-hand area of the screen becomes live.
2. Use the Configure link to the map resource from the protected to the recovery site.
3. Repeat to map all of the appropriate resources.





Creating and configuring protection groups

After configuring inventory mappings, create and configure protection groups. A protection group defines the specific items you want to move from the protected site to the recovery site in the event of a disaster. Such items might include virtual machines (VMs), resource pools, data stores, and networks.

Protection groups can protect VMs, applications, or a combination of the two (for example, an application distributed across multiple VMs).

For ease of management, it is ideal to maintain a one-to-one mapping between SRM protection groups and CLARiiON consistency groups. However, if the number of mirrors you want to have in a single protection group would exceed the maximum number of mirrors permitted in a single consistency group (this number depends on the CLARiiON array model being used), multiple consistency groups can be mapped to a single protection group. Table 4 lists the maximum number of mirrors and consistency groups supported by each CLARiiON model.

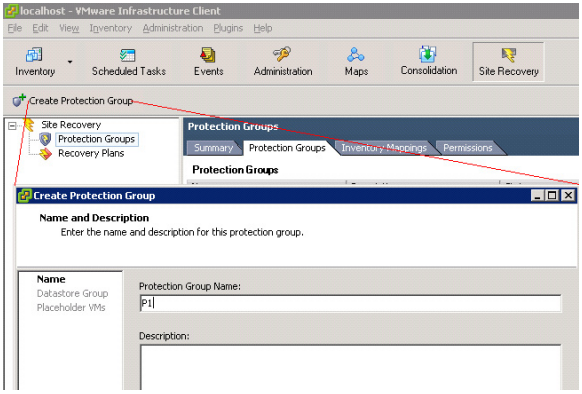
Table 4 Maximum number of mirrors and consistency groups per CLARiiON model

	CX3-10c	CX3-20c, CX3-20f	CX3-40c, CX3-40f, CX3-80
Mirrors per storage system	50 max.	100 max.	200 max.
Mirrors with write intent log per storage system	25 max.	50 max.	100 max.
Mirrors per consistency group	8 max.	8 max.	16 max.
Consistency groups per CLARiiON model	8 max.	8 max.	16 max.

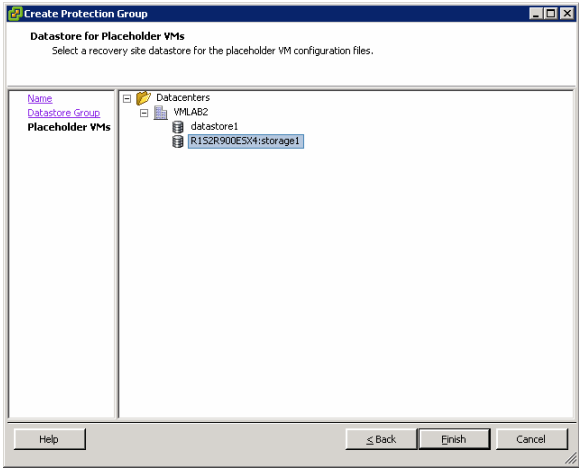
Note: Create and configure protection groups only on the VirtualCenter client connected to the protected site.

To create and configure a protection group, follow the example presented below:

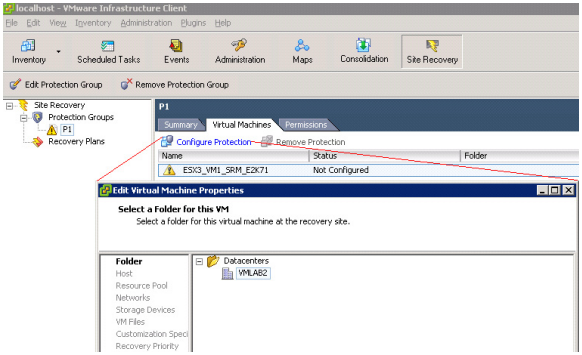
1. In the main window of the VirtualCenter client connected to the protected site, select Create Protection Group.
2. Specify a name for the protection group.
3. Select the VMs to be failed over as a group.
4. Click Next.



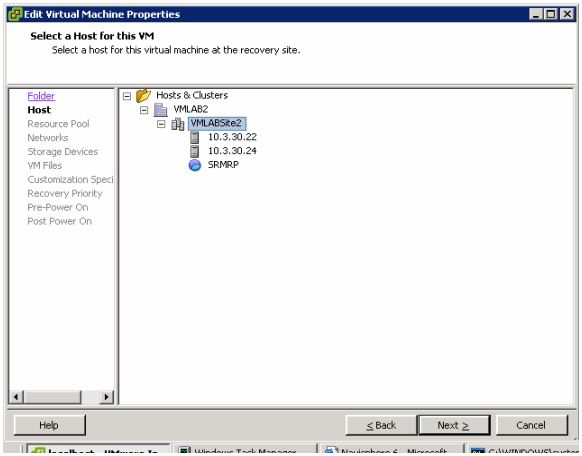
5. Select a recovery site data store for the placeholder VM configuration files.
6. Click Finish.

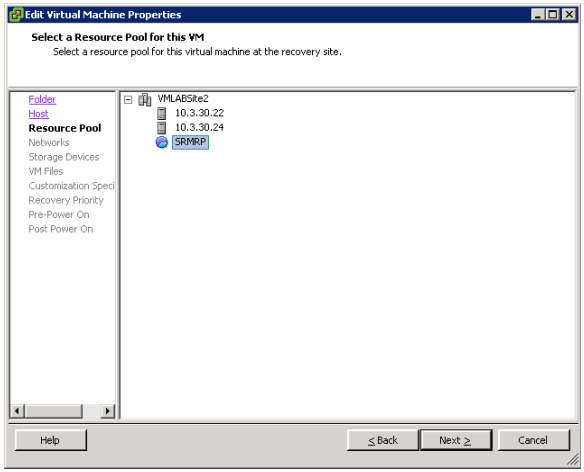


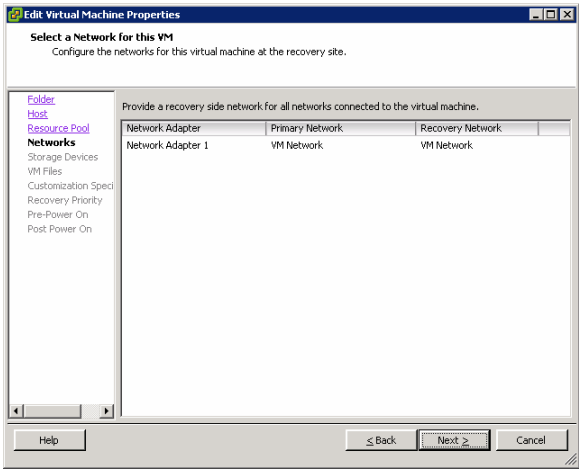
7. In the main window of the VirtualCenter client, select Configure Protection.

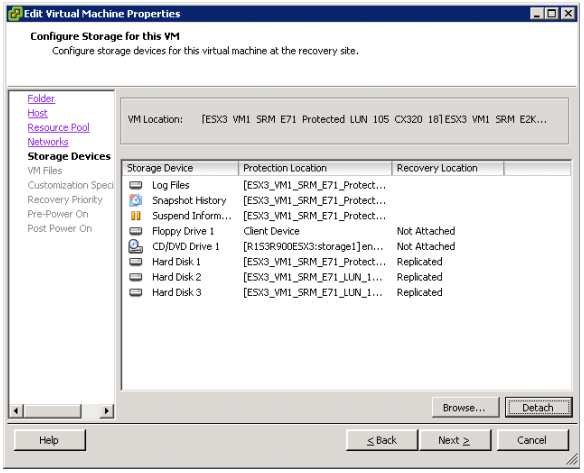


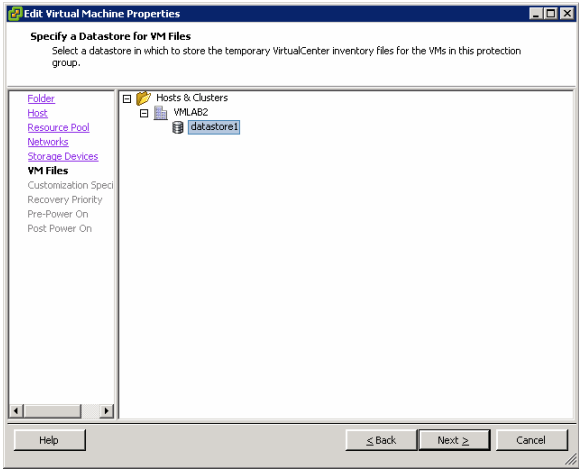
8. Follow the instructions presented by the Edit Virtual Machine Properties wizard, as shown in the following sequence of screenshots.

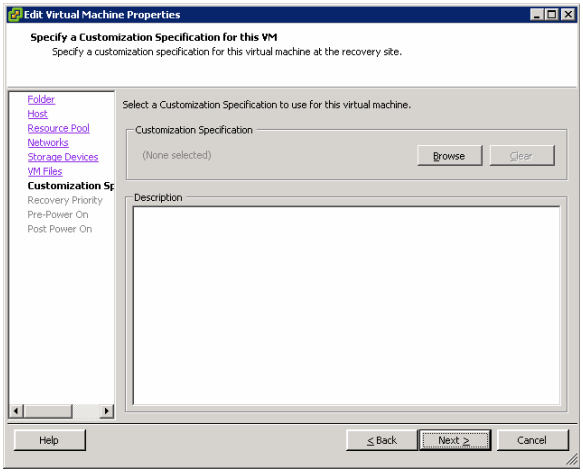


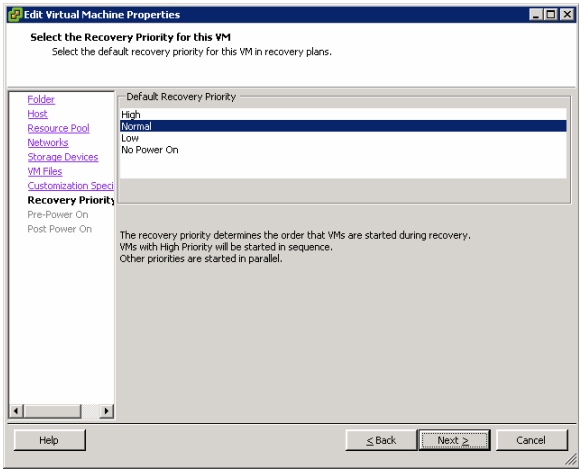

Edit Virtual Machine Properties
Select a Resource Pool for this VM
Select a resource pool for this virtual machine at the recovery site.
Folder
Host
Resource Pool
Networks
Storage Devices
VM Files
Customization Speci
Recovery Priority
Pre-Power On
Post Power On
VMLABSite2
10.3.30.22
10.3.30.24
SRMRP
Help
≤ Back
Next ≥
Cancel

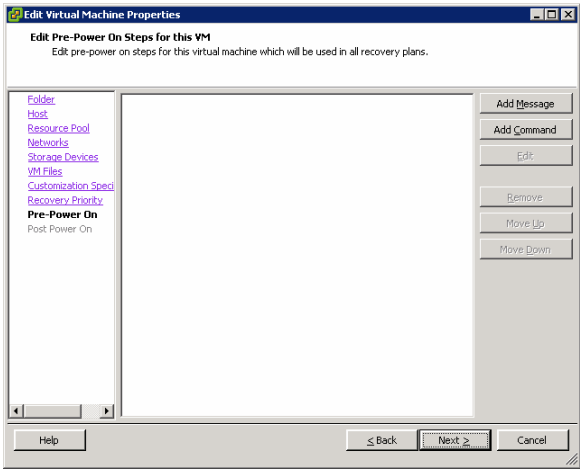

Edit Virtual Machine Properties
Select a Network for this VM
Configure the networks for this virtual machine at the recovery site.
Folder
Host
Resource Pool
Networks
Storage Devices
VM Files
Customization Speci
Recovery Priority
Pre-Power On
Post Power On
Provide a recovery side network for all networks connected to the virtual machine.
Network Adapter
Primary Network
Recovery Network
Network Adapter 1
VM Network
VM Network
Help
≤ Back
Next ≥
Cancel

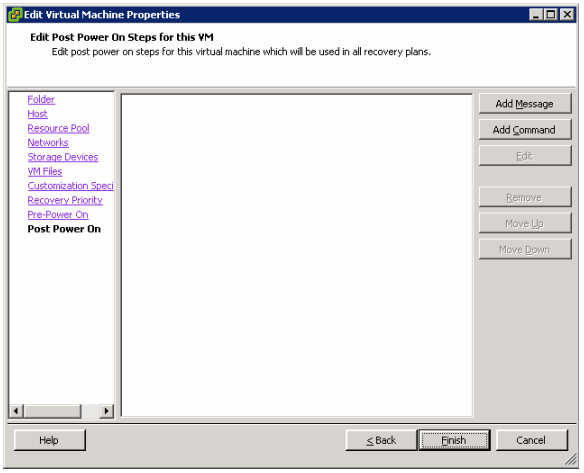

Edit Virtual Machine Properties
Configure Storage for this VM
Configure storage devices for this virtual machine at the recovery site.
Folder
Host
Resource Pool
Networks
Storage Devices
VM Files
Customization Speci
Recovery Priority
Pre-Power On
Post Power On
VM Location: [ESX3_VM1_SRM_E71_Protected_LUN_105_CX320_18]ESX3_VM1_SRM_E2K...
Storage Device
Protection Location
Recovery Location
Log Files
[ESX3_VM1_SRM_E71_Protect...
Snapshot History
[ESX3_VM1_SRM_E71_Protect...
Suspend Inform...
[ESX3_VM1_SRM_E71_Protect...
Floppy Drive 1
Client Device
Not Attached
CD/DVD Drive 1
[R153R900ESX3:storage1]en...
Not Attached
Hard Disk 1
[ESX3_VM1_SRM_E71_Protect...
Replicated
Hard Disk 2
[ESX3_VM1_SRM_E71_LUN_1...
Replicated
Hard Disk 3
[ESX3_VM1_SRM_E71_LUN_1...
Replicated
Browse...
Detach
Help
≤ Back
Next ≥
Cancel


Edit Virtual Machine Properties
Specify a Datastore for VM Files
Select a datastore in which to store the temporary VirtualCenter inventory files for the VMs in this protection group.
Folder
Host
Resource Pool
Networks
Storage Devices
VM Files
Customization Speci
Recovery Priority
Pre-Power On
Post Power On
Hosts & Clusters
VMLAB2
datastore1
Help
≤ Back
Next ≥
Cancel

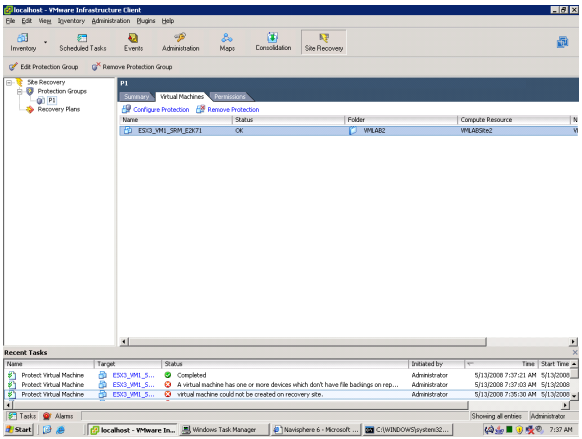

Edit Virtual Machine Properties
Specify a Customization Specification for this VM
Specify a customization specification for this virtual machine at the recovery site.
Folder
Host
Resource Pool
Networks
Storage Devices
VM Files
Customization Sp
Recovery Priority
Pre-Power On
Post Power On
Select a Customization Specification to use for this virtual machine.
Customization Specification
(None selected)
Browse
Clear
Description
Help
< Back
Next >
Cancel


Edit Virtual Machine Properties
Select the Recovery Priority for this VM
Select the default recovery priority for this VM in recovery plans.
Folder
Host
Resource Pool
Networks
Storage Devices
VM Files
Customization Speci
Recovery Priority
Pre-Power On
Post Power On
Default Recovery Priority
High
Normal
Low
No Power On
The recovery priority determines the order that VMs are started during recovery.
VMs with High Priority will be started in sequence.
Other priorities are started in parallel.
Help
< Back
Next >
Cancel


Edit Virtual Machine Properties
Edit Pre-Power On Steps for this VM
Edit pre-power on steps for this virtual machine which will be used in all recovery plans.
Folder
Host
Resource Pool
Networks
Storage Devices
VM Files
Customization Speci
Recovery Priority
Pre-Power On
Post Power On
Add Message
Add Command
Edit
Remove
Move Up
Move Down
Help
< Back
Next >
Cancel


Edit Virtual Machine Properties
Edit Post Power On Steps for this VM
Edit post power on steps for this virtual machine which will be used in all recovery plans.
Folder
Host
Resource Pool
Networks
Storage Devices
VM Files
Customization Speci
Recovery Priority
Pre-Power On
Post Power On
Add Message
Add Command
Edit
Remove
Move Up
Move Down
Help
< Back
Finish
Cancel

9. The protection group is now configured and should appear on the Virtual Machines tab in the main window of the VirtualCenter client. If necessary, repeat steps 1 through 9 to create and configure additional protection groups.



Modifying the protection group configuration

To demonstrate the flexibility of the protection group configuration, the following operations were performed as part of the lab-based implementation scenario:

- Adding an extent to a VMFS data store by presenting a new LUN to the VMware ESX server (see below for steps)
- Extending a LUN as a metaLUN (not described in this document)

Adding an extent to a VMFS data store

The following steps were performed to add an extent to a VMFS data store by presenting a new LUN to the VMware ESX server:

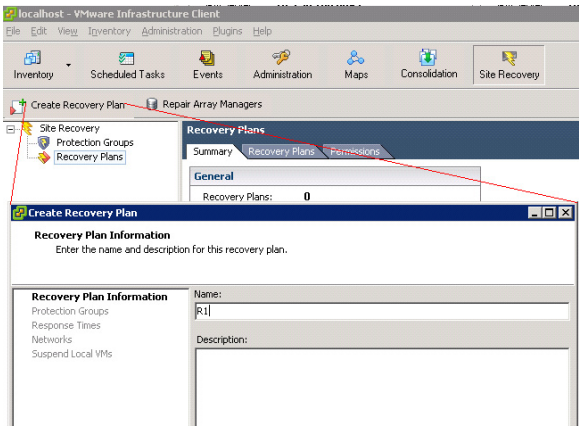
1. Add a new mirror LUN to a consistency group.
2. Add the new LUN to the protected array's storage group.
3. Add the secondary image to the recovery array's storage group.
4. Create snapshots and ensure the is recovery plan is available.
5. Using the VMware VirtualCenter client, extend the VMFS datastore by adding an extent.
6. Using Array Manager, rescan the arrays so that the new LUN is added to the LUN count number.

Creating a recovery plan

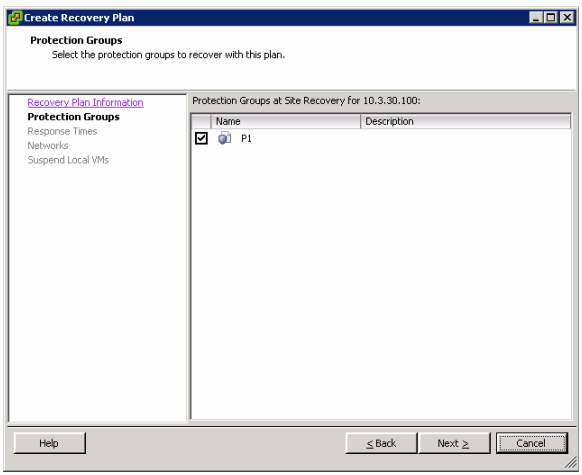
After creating and configuring protection groups, create a recovery plan as shown in the example below.

Note: Create the recovery plan on the VirtualCenter client connected to the recovery site.

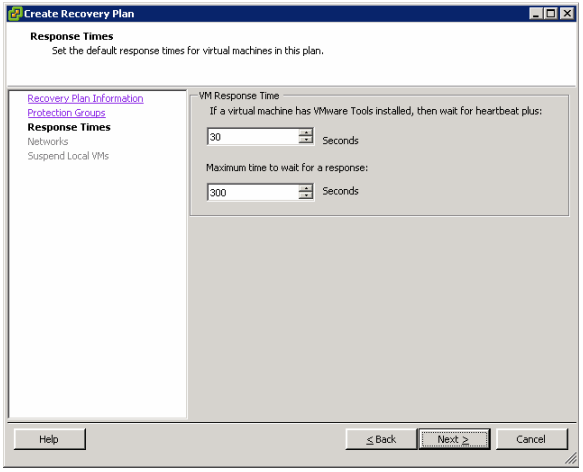
1. From the VirtualCenter client connected to the recovery site, click Create Recovery Plan.

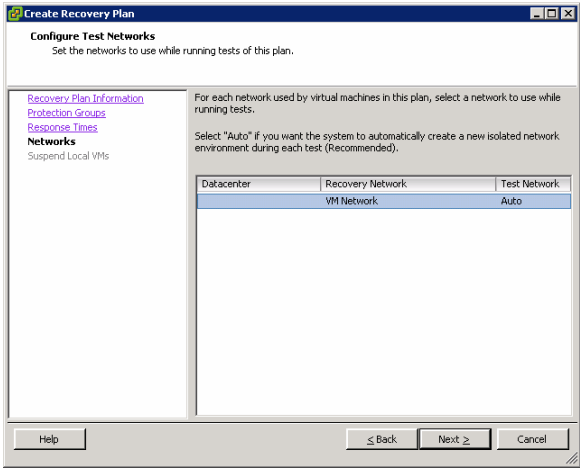


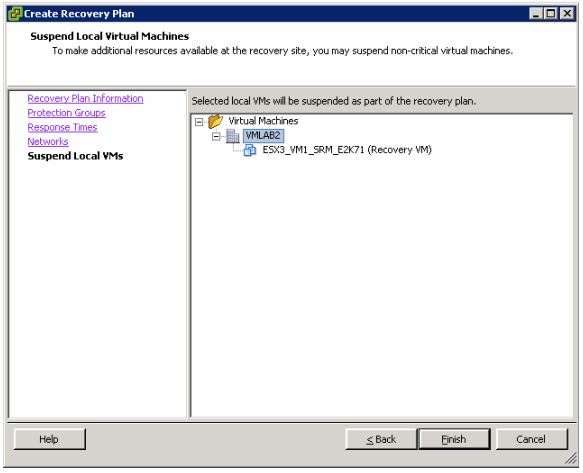
2. Select the protection group you previously created and click Next.



3. Continue to follow the instructions that the wizard presents.







3 Validation

This chapter includes the following topics:

Testing the recovery plan

After creating an SRM recovery plan, it is important to test the plan to verify that it is performing the expected operations.

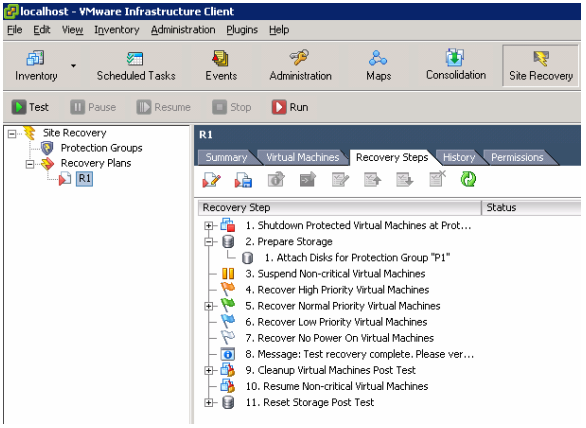
SRM provides the ability to test a recovery plan from the recovery site. When running a test, SRM executes the configured recovery plan with the following exceptions:

- The recovery site does not connect to the production site and does not shut down the production VMs.
- During a test, a test network is created at the recovery site so that the infrastructure of the recovery site is not affected. The test network is deleted at the conclusion of the test.

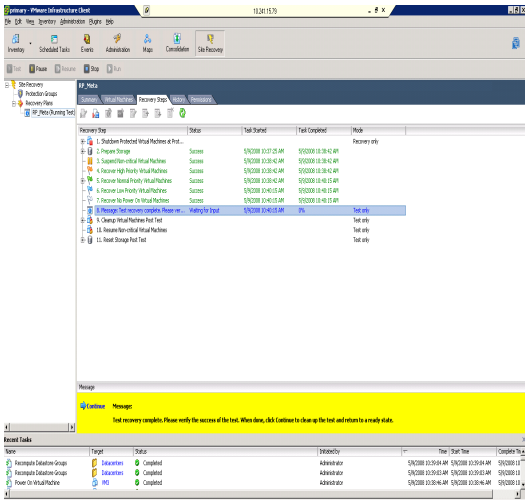
Note: Recovery plans are tested only from the VirtualCenter client connected to the recovery site.

To test the recovery plan you previously created:

1. From the VirtualCenter client connected to the recovery site, open the recovery plan you previously created and configured.
2. Select the Recovery Steps tab to view the sequence of configured events.
3. Click Test. SRM begins to execute the recovery plan in test mode.



4. The following events occur:
   a. CLARiiON SnapView sessions are started and activated against the snapshots.
   b. SRM simulates the carry-over of all of the resources created within the SRM protection group to the recovery site.
   c. The recovery VMs are powered on in the order defined within the recovery plan.
   d. SRM pauses.



5. Open a console for a VM that was started at the recovery site and verify that the data is as you would expect it to be.
6. Click the Continue button to have SRM clean up the test and revert back to the original production state.

See also For additional information about testing SRM recovery plans, refer to the *Administration Guide for Site Recovery Manager*, available on the VMware website (http://www.VMware.com).

Recovery plan execution operations

Executing an SRM recovery plan is similar to testing a recovery plan with the following differences:

- Executing a recovery plan is a one-time activity; testing a recovery plan can be performed multiple times.
- When a recovery plan is executed, SnapView snapshots are not involved. Instead, the MirrorView/S recovery copies are promoted to be the new protected LUNs for production operation.
- When a recovery plan is executed, the remote copy becomes the production copy and vice versa. Testing a recovery plan does not transfer production to the remote copy.

- After executing a recovery plan, manual steps are required to resume operation at the original production site. Testing a recovery plan does not require such steps because production is not actually transferred to the remote site.

Note: Recovery plans are executed from the VirtualCenter client connected to the recovery site.

Important: Executing an SRM recovery plan should be done only in the event of a declared disaster to enable operations to be resumed at the recovery site.

Recovery plan execution scenarios

The following recovery plan execution scenarios were conducted as part of validation. All scenarios were successful.

- A single recovery plan with single protection group.
- A single recovery plan with multiple protection groups.
- Multiple recovery plans having the same protection group or groups. Tests could be run only one at a time, and each test had to complete before the next test could be started.
- Multiple recovery plans with a single protection group or multiple protection groups. Each recovery plan used a unique protection group; that is, a given protection group was used in one (and only one) recovery plan. Tests had to be staggered, meaning that one plan's test had to progress to the point of the snapshots becoming active on the recovery site before the next plan's test could begin.

Note: Recovery plan tests completed even if the mirrors were system-fractured or administratively fractured. Note also that recovery plan tests verify only that the mirror snapshots are configured properly and can be mounted using VMs.

Failover operations

The following failover operations were conducted as part of validation:

- Failing over with all mirrors in active synchronization

- Failing over with an administrative fracture (not described in this document). Note that, even though failover was successful, the risk is that the recovery copy might not have received all of the data that was written to the production (protected site) LUN.
- Failing over with a system fracture. The VirtualCenter client and the array at the protected site was powered down and the recovery plan was executed. The VMs were successfully brought up on the recovery site.

Note: Failover operations are initiated from the VirtualCenter client connected to the recovery site.

Failback operations

The extent of a disaster determines whether recovery is performed to a newly provisioned site or to the original site. Thus, different steps are required depending on the scenario. However, the underlying technology and initialization of SRM are the same.

Note: Failback operations are initiated from the VirtualCenter client connected to the *original* protected site.

The general steps required for failback are as follows:

1. Perform cleanup with VirtualCenter:
   a. Remove the VMs from inventory on the protected site.
   b. Remove the failed-over recovery plan from the recovery site.
   c. Remove the protection group or groups associated with the removed recovery plan from the protected site.
2. Depending on the state of the mirrors at the time of failover (for example, system-fractured), MirrorView replication must be reversed in some fashion to perform replication in the opposite direction (recovery site to protected site). For instructions on addressing various failback scenarios with MirrorView, refer to the *EMC MirrorView Adapter for VMware Site Recovery Manager Release Notes*.

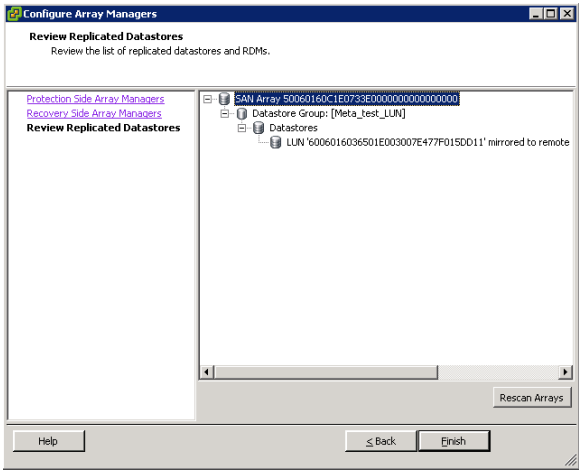
3. Configure SRM to fail back from the recovery site. Using SRM Array Manager, perform the following steps on both arrays:

   a. Add the recovery array as the new protected array (only if it has not yet been added).

   b. Add the protected array as the new recovery array (only if it has not yet been added).

   c. (Optional) Remove the previous protected/recovery array configuration.

   d. Rescan the arrays. The data sources to fail back should now be displayed.



4. Close and reopen the VirtualCenter client.
5. Re-create the protection group or groups on the new protected array (previously the recovery array).
6. Re-create the recovery plan on the new recovery array (previously the protected array).
7. Test the recovery plan.
8. Initiate failover from the new protected array to the new recovery array.
9. Repeat steps 1 through 7 to revert the environment to SRM readiness.

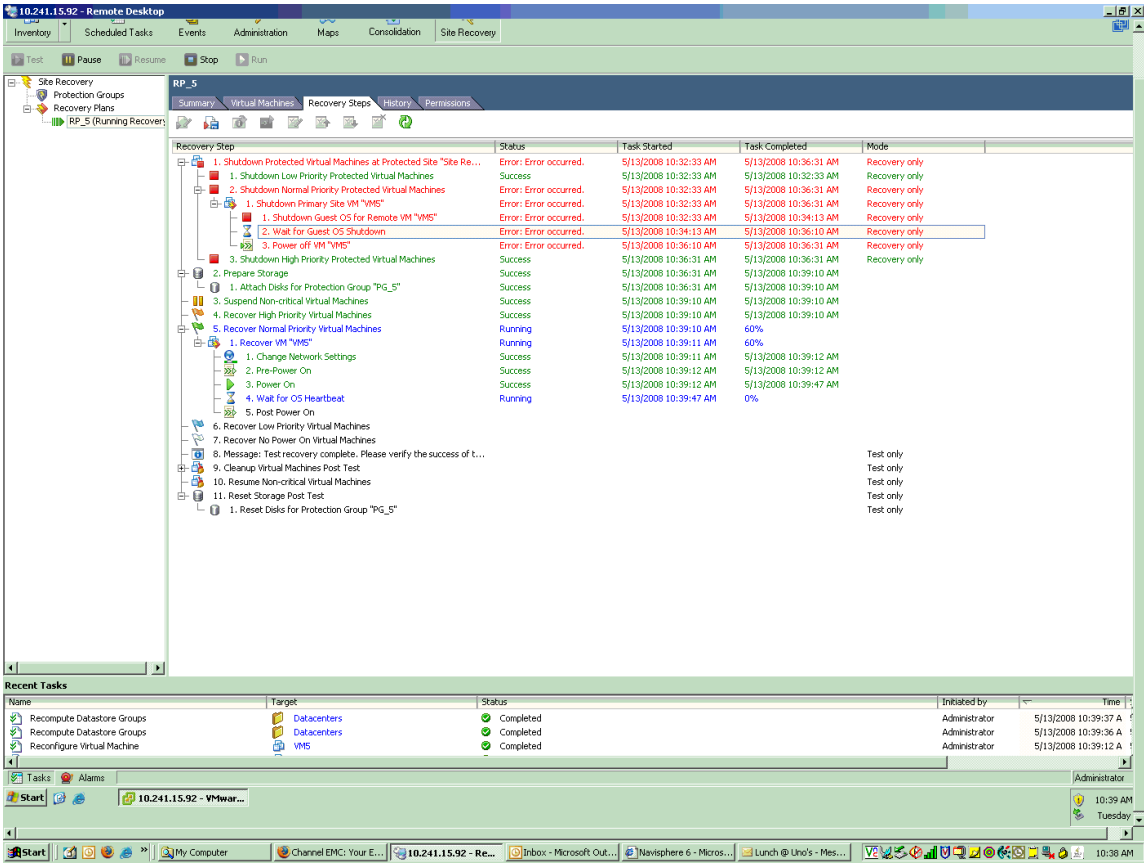
4 Recommendations and Conclusion

This chapter includes the following topics:

Recommendations

As a direct result of working through this implementation scenario, the solution architects identified the following recommendations.

- If the VMs to be failed over do not have VMware Tools installed, the recovery plan will generate an error when attempting to shut down the production VMs (notice the step that is annotated in the screenshot below). The remaining steps in the plan will succeed, however, provided the plan was configured properly. The final status of the recovery plan will display the error (on the History tab), even if the VMs failed over successfully.



- SnapView must be enabled on the arrays and snapshots at both the protected and recovery sites to enable testing of failover and failback.
- Alarms should be created to announce the creation of new VMs on the data store, so that mirrors can be configured to include the new VMs in the SRM protection scheme.
- It is strongly recommended that CLARiiON-side configurations be completed (setting up MirrorView, creating snapshots, and so on) before installing SRM and SRA.
- If SRM is used for failover, it is recommended that SRM also be used for failback, since manual failback is cumbersome and requires changing the LVMEnableresignature on the protected ESX servers. By default, SRM changes the LVMEnableresignature to 1 and then renames the VMFS data stores.
- Testing of a recovery plan captures only snapshots of the MirrorView secondary image and does not verify whether there is connectivity between the arrays or whether MirrorView is working properly. To verify connectivity between VM consoles, use the SRM connection. To verify connectivity between arrays, use SRM Array Manager or Navisphere Manager.
- Ensure that you have enough disk space configured for the VM and swap file at the recovery site to ensure that the recovery plan test runs successfully and without errors.

Conclusion

This guide provided an illustrated walkthrough, with example screenshots and command line input, of the processes of setting up and testing a disaster recovery plan using SRM for ESX Server 3.5 virtual machines with EMC MirrorView/S and CLARiiON CX3 storage systems. Also included were a limited set of recommendations for individuals attempting to implement such a solution in the field.