

vmware® PRESS



# Administering VMware Site Recovery Manager 5.0

TECHNOLOGY HANDS-ON

**Mike Laverick**



# **Administering VMware Site Recovery Manager 5.0**

VMware Press is the official publisher of VMware books and training materials, which provide guidance on the critical topics facing today's technology professionals and students. Enterprises, as well as small- and medium-sized organizations, adopt virtualization as a more agile way of scaling IT to meet business needs. VMware Press provides proven, technically accurate information that will help them meet their goals for customizing, building, and maintaining their virtual environment.

With books, certification and study guides, video training, and learning tools produced by world-class architects and IT experts, VMware Press helps IT professionals master a diverse range of topics on virtualization and cloud computing and is the official source of reference materials for preparing for the VMware Certified Professional Examination.

VMware Press is also pleased to have localization partners that can publish its products into more than forty-two languages, including, but not limited to, Chinese (Simplified), Chinese (Traditional), French, German, Greek, Hindi, Japanese, Korean, Polish, Russian, and Spanish.

For more information about VMware Press please visit

**<http://www.vmware.com/go/vmwarepress>**

# Administering VMware Site Recovery Manager 5.0

TECHNOLOGY HANDS-ON

Mike Laverick

**vmware**® PRESS

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco  
New York • Toronto • Montreal • London • Munich • Paris • Madrid  
Capetown • Sydney • Tokyo • Singapore • Mexico City

## Administering VMware Site Recovery Manager 5.0

Copyright © 2012 VMware, Inc.

Published by Pearson Education, Inc.

Publishing as VMware Press

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. To obtain permission to use material from this work, please submit a written request to Pearson Education, Inc., Permissions Department, One Lake Street, Upper Saddle River, New Jersey 07458, or you may fax your request to (201) 236-3290.

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. The publisher cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

VMware terms are trademarks or registered trademarks of VMware in the United States, other countries, or both.

### Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author, VMware Press, VMware and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

The opinions expressed in this book belong to the author and are not necessarily those of VMware.

### Corporate and Government Sales

VMware Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact U.S. Corporate and Government Sales, (800) 382-3419, [corpsales@pearsontechgroup.com](mailto:corpsales@pearsontechgroup.com). For sales outside the United States, please contact International Sales, [international@pearson.com](mailto:international@pearson.com).

*Library of Congress Control Number:* 2011919183

ISBN-13: 978-0-321-79992-0

ISBN-10: 0-321-79992-5

Text printed in the United States on recycled paper at RR Donnelley in Crawfordsville, Indiana.

First printing, December 2011

VMWARE PRESS  
PROGRAM MANAGER  
Andrea Eubanks  
de Jounge

ASSOCIATE PUBLISHER  
David Dusthimer

ACQUISITIONS EDITOR  
Joan Murray

DEVELOPMENT EDITOR  
Susan Zahn

MANAGING EDITOR  
John Fuller

FULL-SERVICE  
PRODUCTION MANAGER  
Julie B. Nahil

COPY EDITOR  
Audrey Doyle

PROOFREADER  
Kelli M. Brooks

INDEXER  
Jack Lewis

EDITORIAL ASSISTANT  
Vanessa Evans

BOOK DESIGNER  
Gary Adair

COMPOSITOR  
Kim Arney

*This book is dedicated to Carmel—for putting up with me and my endless ramblings about virtualization.*

*This page intentionally left blank*

# Contents

**Preface xv**

**Acknowledgments xxi**

**About the Author xxiii**

## **1 Introduction to Site Recovery Manager 1**

What's New in Site Recovery Manager 5.0	1
vSphere 5 Compatibility	2
vSphere Replication	2
Automated Failback and Reprotect	3
VM Dependencies	4
Improved IP Customization	4
A Brief History of Life before VMware SRM	5
What Is Not a DR Technology?	7
vMotion	7
VMware HA Clusters	8
VMware Fault Tolerance	9
Scalability for the Cloud	9
What Is VMware SRM?	10
What about File Level Consistency?	11
Principles of Storage Management and Replication	12
Caveat #1: All Storage Management Systems Are the Same	12
Caveat #2: All Storage Vendors Sell Replication	13
Caveat #3: Read the Manual	14
Summary	19

## **2 Getting Started with Dell EqualLogic Replication 21**

Creating an EqualLogic iSCSI Volume	23
Granting ESXi Host Access to the EqualLogic iSCSI Volume	26
Enabling Replication for EqualLogic	31
Configuring Replication Partners	32
Configuring Replication of the iSCSI Volume	34
Configuring a Schedule for Replication	37
Using EqualLogic Host Integration for VMware Edition (HIT-VE)	39
Summary	42



**3 Getting Started with EMC Celerra Replication 43**

- Creating an EMC Celerra iSCSI Target 46
- Granting ESX Host Access to the EMC Celerra iSCSI Target 51
- Creating a New File System 56
- Creating an iSCSI LUN 59
- Configuring Celerra Replication 64
- Summary 72

**4 Getting Started with EMC CLARiiON MirrorView 73**

- Creating a Reserved LUN Pool 75
- Creating an EMC LUN 78
- Configuring EMC MirrorView 80
- Creating a Snapshot for SRM Tests 85
- Creating Consistency Groups (Recommended) 88
- Granting ESX Host Access to CLARiiON LUNs 90
  - At the Recovery Site CLARiiON (New Jersey) 90
  - At the Protected Site CLARiiON (New York) 91
- Using the EMC Virtual Storage Integrator Plug-in (VSI) 93
- Summary 95

**5 Getting Started with the HP StorageWorks P4000 Virtual SAN Appliance with Remote Copy 97**

- Some Frequently Asked Questions about the HP P4000 VSA 98
- Downloading and Uploading the VSA 100
  - Importing the StorageWorks P4000 VSA 100
  - Modifying the VSA's Settings and First-Power-On Configuration 103
  - Primary Configuration of the VSA Host 105
  - Installing the Management Client 107
- Configuring the VSA (Management Groups, Clusters, and Volumes) 108
  - Adding the VSAs to the Management Console 108
  - Adding the VSAs to Management Groups 108
  - Creating a Cluster 111
  - Creating a Volume 112
  - Licensing the HP VSA 113
  - Configuring the HP VSA for Replication 114
  - Monitoring Your Replication/Snapshot 118
- Adding ESX Hosts and Allocating Volumes to Them 120
  - Adding an ESX Host 120
  - Allocating Volumes to ESX Hosts 120
  - Granting ESX Host Access to the HP VSA iSCSI Target 122

---

Monitoring Your iSCSI Connections	127
The HP StorageWorks P4000 VSA: Creating a Test Volume at the Recovery Site	127
Shutting Down the VSA	129
Summary	129

## **6 Getting Started with NetApp SnapMirror 131**

Provisioning NetApp NFS Storage for VMware ESXi	133
Creating a NetApp Volume for NFS	134
Granting ESXi Host Access to NetApp NFS Volumes	137
Creating NetApp Volumes for Fibre Channel and iSCSI	139
Granting ESXi Host Access to the NetApp iSCSI Target	142
Configuring NetApp SnapMirror	147
Confirm IP Visibility (Mandatory) and Name Resolution (Optional)	147
Enable SnapMirror (Both the Protected and Recovery Filers)	148
Enable Remote Access (Both the Protected and Recovery Filers)	148
Configure SnapMirror on the Recovery Site NetApp Filer (New Jersey)	150
Introducing the Virtual Storage Console (VSC)	155
Summary	158

## **7 Installing VMware SRM 161**

Architecture of the VMware SRM	161
Network Communication and TCP Port Numbers	161
Storage Replication Components	164
VMware Components	166
More Detailed Information about Hardware and Software Requirements	169
Scalability of VMware SRM	171
Designed for Both Failover and Failback?	172
A Word about Resignaturing VMFS Volumes	173
VMware SRM Product Limitations and Gotchas	178
Licensing VMware SRM	179
Setting Up the VMware SRM Database with Microsoft SQL Server 2008	180
Creating the Database and Setting Permissions	181
Configuring a DSN Connection on the SRM Server(s)	184
Installing the VMware SRM Server	186
Installing the SRM Software	186
Installing a Storage Replication Adapter: Example HP SRA	193
Installing the vSphere Client SRM Plug-in	195
Handling Failures to Connect to the SRM Server	198
Summary	199

## **8 Configuring vSphere Replication (Optional) 201**

- How vSphere Replication Works 201
- vSphere Replication Limitations 203
- Installing vSphere Replication 205
  - Setting the vCenter Managed IP Address 205
  - Configuring a Database for the VRMS 206
  - Deploying the VRMS 208
  - Configuring the VRMS 212
  - Configuring the VRMS Connection 214
  - Deploying the VRS 215
  - Registering the VRS 216
- Enabling and Monitoring vSphere Replication 217
  - Moving, Pausing, Resuming, Removing, and Forcing Synchronization 220
  - Enabling Replication for Physical Couriering 220
  - Configuring Datastore Mappings 221
- Summary 223

## **9 Configuring the Protected Site 225**

- Connecting the Protected and Recovery Site SRMs 226
- Configuring Inventory Mappings 231
  - Configuring Resource Mappings 234
  - Configuring Folder Mappings 235
  - Configuring Network Mappings 236
- Assigning Placeholder Datastores 237
- Configuring Array Managers: An Introduction 241
  - Configuring Array Managers: Dell EqualLogic 245
  - Configuring Array Managers: EMC Celerra 248
  - Configuring Array Managers: EMC CLARiiON 251
  - Configuring Array Managers: NetApp FSA 254
- Creating Protection Groups 257
- Failure to Protect a Virtual Machine 262
  - Bad Inventory Mappings 262
  - Placeholder VM Not Found 264
  - VMware Tools Update Error—Device Not Found: CD/DVD Drive 1 265
  - Delete VM Error 266
  - It's Not an Error, It's a Naughty, Naughty Boy! 266
- Summary 267

---

## 10 Recovery Site Configuration 269

- Creating a Basic Full-Site Recovery Plan 269
- Testing Storage Configuration at the Recovery Site 273
  - Overview: First Recovery Plan Test 275
- Practice Exercise: First Recovery Plan Test 281
- Cleaning Up after a Recovery Plan Test 283
- Controlling and Troubleshooting Recovery Plans 285
  - Pause, Resume, and Cancel Plans 285
  - Error: Cleanup Phase of the Plan Does Not Always Happen with iSCSI 287
  - Error: Loss of the Protection Group Settings 288
  - Error: Cleanup Fails; Use Force Cleanup 289
  - Error: Repairing VMs 290
  - Error: Disconnected Hosts at the Recovery Site 290
- Recovery Plans and the Storage Array Vendors 291
  - Dell EqualLogic and Testing Plans 291
  - EMC Celerra and Testing Plans 292
  - NetApp and Testing Plans 294
- Summary 295

## 11 Custom Recovery Plans 297

- Controlling How VMs Power On 299
  - Configuring Priorities for Recovered Virtual Machines 299
  - Adding VM Dependencies 302
  - Configuring Start-Up and Shutdown Options 305
  - Suspending VMs at the Recovery Site 308
- Adding Additional Steps to a Recovery Plan 309
  - Adding Prompt Steps 309
  - Adding Command Steps 313
  - Adding Command Steps with VMware PowerCLI 315
  - Managing PowerCLI Authentication and Variables 321
  - Adding Command Steps to Call Scripts within the Guest Operating System 328
- Configuring IP Address Changes for Recovery Virtual Machines 329
  - Creating a Manual IP Guest Customization 330
  - Configuring Bulk IP Address Changes for the Recovery Virtual Machine (dr-ip-exporter) 332
  - Creating Customized VM Mappings 336
- Managing Changes at the Protected Site 337
  - Creating and Protecting New Virtual Machines 337
  - Renaming and Moving vCenter Inventory Objects 338

Other Objects and Changes in the vSphere and SRM Environment	342
Storage vMotion and Protection Groups	343
Virtual Machines Stored on Multiple Datastores	346
Virtual Machines with Raw Device/Disk Mappings	348
Multiple Protection Groups and Multiple Recovery Plans	350
Multiple Datastores	350
Multiple Protection Groups	351
Multiple Recovery Plans	352
The Lost Repair Array Managers Button	354
Summary	354

## **12 Alarms, Exporting History, and Access Control 357**

vCenter Linked Mode and Site Recovery Manager	357
Alarms Overview	360
Creating a New Virtual Machine to Be Protected by an Alarm (Script)	362
Creating a Message Alarm (SNMP)	364
Creating an SRM Service Alarm (SMTP)	364
Exporting and History	366
Exporting Recovery Plans	366
Recovery Plan History	367
Access Control	368
Creating an SRM Administrator	370
Summary	372

## **13 Bidirectional Relationships and Shared Site Configurations 375**

Configuring Inventory Mappings	376
Refreshing the Array Manager	378
Creating the Protection Group	380
Creating the Recovery Plan	381
Using vApps to Control Start-Up Orders	381
Shared Site Configurations	384
Installing VMware SRM with Custom Options to the New Site (Washington DC)	387
Installing VMware SRM Server with Custom Options to the Recovery Site	390
Pairing the Sites Together	392
Decommissioning a Site	394
Summary	394

---

## 14 Failover and Failback 397

- Planned Failover: Protected Site Is Available 400
  - Dell EqualLogic and Planned Recovery 404
  - NetApp and Planned Recovery 405
  - Automated Failback from Planned Migration 407
- Unplanned Failover 415
  - Protected Site Is Dead 415
  - Planned Failback after a Disaster 419
- Summary 421

## 15 Scripting Site Recovery 423

- Scripted Recovery for a Test 425
  - Managing the Storage 425
  - Rescanning ESX Hosts 426
  - Resignaturing VMFS Volumes 427
  - Mounting NFS Exports 428
  - Creating an Internal Network for the Test 428
  - Adding Virtual Machines to the Inventory 429
  - Fixing VMX Files for the Network 430
- Summary 432

## 16 Upgrading from SRM 4.1 to SRM 5.0 433

- Upgrading vSphere 435
  - Step 1: Run the vCenter Host Agent Pre-Upgrade Checker 436
  - Step 2: Upgrade vCenter 436
  - Step 3: Upgrade the vCenter Client 441
  - Step 4: Upgrade the VMware Update Manager (VUM) 442
  - Step 5: Upgrade the VUM Plug-in 443
  - Step 6: Upgrade Third-Party Plug-ins (Optional) 445
  - Step 7: Upgrade the ESX Hosts 445
- Upgrading Site Recovery Manager 451
  - Step 8: Upgrade SRM 452
  - Step 9: Upgrade VMware Tools (Optional) 455
  - Step 10: Upgrade Virtual Hardware (Optional) 458
  - Step 11: Upgrade VMFS Volumes (Optional) 460
  - Step 12: Upgrade Distributed vSwitches (Optional) 462
- Summary 463

## Index 465

*This page intentionally left blank*

# Preface

This edition of *Administering VMware Site Recovery Manager 5.0* is not only a new edition of this book but one of the first books published by VMware Press.

## About This Book

Version 5.0 represents a major milestone in the development of VMware Site Recovery Manager (SRM). The need to write a book on SRM 5.0 seems more pressing than ever because of the many new features and enhancements in this version. I think these enhancements are likely to draw to the product a whole new raft of people who previously may have overlooked it. Welcome to the wonderful world that is Site Recovery Manager!

This is a complete guide to using SRM. The version of both ESX and vCenter that we use in the book is 5.0. This book was tested against the ESX5i release. This is in marked contrast to the first edition of this book and the SRM product where ESXi was not initially supported. In the previous edition of the book I used abstract names for my vCenter structures, literally calling the vCenter in the Protected Site virtualcenterprotectedsite.rtfm-ed.co.uk. Later I used two cities in the United Kingdom (London and Reading) to represent a Protected Site and a Recovery Site. This time around I have done much the same thing. But the protected location is New York and the recovery location is New Jersey. I thought that as most of my readers are from the United States, and there isn't a person on the planet who hasn't heard of these locations, people would more quickly latch on to the scenario. Figure P.1 shows my structure, with one domain (corp.com) being used in New York and New Jersey. Each site has its own Microsoft Active Directory domain controller, and there is a router between the sites. Each site

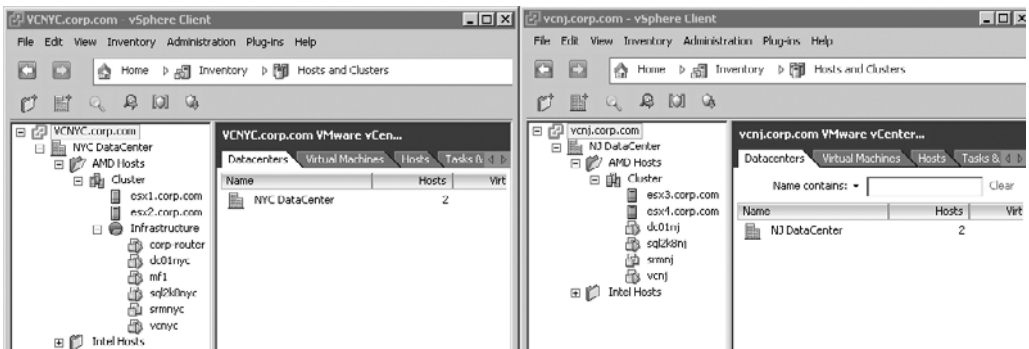


Figure P.1 Two vCenter environments side by side



has its own vCenter, Microsoft SQL Server 2008, and SRM Server. In this case I chose not to use the linked mode feature of vCenter 5; I will introduce that configuration later in the book. I made this decision merely to keep the distinction clear: that I have two separate locations or sites.

## You, the Reader

I have a very clear idea of the kind of person reading this book. Ideally, you have been working with VMware vSphere for some time—perhaps you have attended an authorized course in vSphere 4 such as the “Install, Configure and Manage” class, or even the “Fast Track” class. On top of this, perhaps you have pursued VMware Certified Professional (VCP) certification. So, what am I getting at? This is not a dummy’s or idiot’s guide to SRM. You are going to need some background, or at least read my other guides or books, to get up to speed. Apart from that, I will be gentle with you—assuming that you have forgotten some of the material from those courses, such as VMFS metadata, UUIDs, and VMFS resignaturing, and that you just have a passing understanding of storage replication.

Finally, the use of storage products in this book shouldn’t be construed as a recommendation of any particular vendor. I just happened to meet the HP LeftHand Networks guys at VMworld Europe 2008 – Cannes. They very kindly offered to give me two NFR licenses for their storage technologies. The other storage vendors who helped me while I was writing this book have been equally generous. In 2008, both Chad Sakac of EMC and Vaughn Stewart of NetApp arranged for my lab environment to be kitted out in the very latest versions of their CLARiiON/Celerra and NetApp FSA systems. This empowered me to be much more storage-neutral than I was in previous editions of this book. For this version of the book I was fortunate to also add coverage of the Dell EqualLogic system. Toward that end, I would like to thank Dylan Locsin and William Urban of Dell for their support.

## What This Book Covers

Here is a quick rundown of what is covered in *Administering VMware Site Recovery Manager 5.0*.

- Chapter 1, Introduction to Site Recovery Manager

This chapter provides a brief introduction to Site Recovery Manager and discusses some use cases.

- Chapter 2, Getting Started with Dell EqualLogic Replication  
This chapter guides readers through the configuration of replication with Dell EqualLogic arrays, and covers the basic configuration of the ESXi iSCSI initiator.
- Chapter 3, Getting Started with EMC Celerra Replication  
This chapter guides readers through the configuration of replication with EMC Celerra arrays, and covers the basic configuration of the ESXi iSCSI initiator.
- Chapter 4, Getting Started with EMC CLARiiON MirrorView  
This chapter guides readers through the configuration of replication with CLARiiON arrays.
- Chapter 5, Getting Started with the HP StorageWorks P4000 Virtual SAN Appliance with Remote Copy  
This chapter guides readers through the configuration of replication with the HP P4000 VSA, and covers the basic configuration of the ESXi iSCSI initiator.
- Chapter 6, Getting Started with NetApp SnapMirror  
This chapter guides readers through the configuration of NetApp replication arrays, and covers configuration for FC, iSCSI, and NFS.
- Chapter 7, Installing VMware SRM  
This chapter covers the installation of VMware Site Recovery Manager, and details post-configuration steps such as installing an array vendor's Site Recovery Adapter software.
- Chapter 8, Configuring vSphere Replication (Optional)  
This optional chapter details the steps required to configure vSphere Replication (VR).
- Chapter 9, Configuring the Protected Site  
This chapter covers the initial setup of the Protected Site and deals with such steps as pairing the sites, inventory mappings, array manager configuration, and placeholder datastore configuration. It also introduces the concept of the SRM Protection Group.
- Chapter 10, Recovery Site Configuration  
This chapter covers the basic configuration of the Recovery Plan at the Recovery Site.

- Chapter 11, Custom Recovery Plans

This chapter discusses how Recovery Plans can have very detailed customization designed around a business need. It also explains the use of message prompts, command steps, and the re-IP of virtual machines.

- Chapter 12, Alarms, Exporting History, and Access Control

This chapter outlines how administrators can configure alarms and alerts to assist in the day-to-day maintenance of SRM. It details the reporting functionality available in the History components. Finally, it covers a basic delegation process to allow others to manage SRM without using built-in permission assignments.

- Chapter 13, Bidirectional Relationships and Shared Site Configurations

The chapter outlines more complicated SRM relationships where SRM protects VMs at multiple sites.

- Chapter 14, Failover and Failback

This chapter covers the real execution of a Recovery Plan, rather than merely a test. It details the planned migration and disaster recovery modes, as well as outlining the steps required to failback VMs to their original locale.

- Chapter 15, Scripting Site Recovery

This chapter covers what to do if Site Recovery Manager is not available. It discusses how to do *manually* everything that Site Recovery Manager automates.

- Chapter 16, Upgrading from SRM 4.1 to SRM 5.0

This chapter offers a high-level view of how to upgrade SRM 4.1 to SRM 5.0. It also covers upgrading the dependencies that allow SRM 5.0 to function, including upgrading ESX, vCenter, Update Manager, and virtual machines.

## Hyperlinks

The Internet is a fantastic resource, as we all know. However, printed hyperlinks are often quite lengthy, are difficult to type correctly, and frequently change. I've created a very simple Web page that contains all the URLs in this book. I will endeavor to keep this page up to date to make life easy for everyone concerned. The single URL you need for all the links and online content is

- [www.rtfm-ed.co.uk/srm.html](http://www.rtfm-ed.co.uk/srm.html)

Please note that depending on when you purchased this book, the location of my resource blog might have changed. Beginning in late January 2012, I should have a new blog for you to access all kinds of virtualization information:

- [www.mikelaverick.com](http://www.mikelaverick.com)

At the time of this writing, there are still a number of storage vendors that have yet to release their supporting software for VMware Site Recovery Manager. My updates on those vendors will be posted to this book's Web page:

- <http://informit.com/title/9780321799920>

## **Author Disclaimer**

No book on an IT product would be complete without a disclaimer. Here is mine: Although every precaution has been taken in the preparation of this book, the contributors and author assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein. Phew, glad that's over with!

Thank you for buying this book. I know I'm not quite James Joyce, but I hope that people find reading this book both entertaining and instructive.

*This page intentionally left blank*

## Acknowledgments

Before we move on to Chapter 1, I would like to thank the many people who helped me as I wrote this book. First, I would like to thank Carmel Edwards, my partner. She puts up with my ranting and raving about VMware and virtualization. Carmel is the first to read my work and did the first proofread of the manuscript.

Second, I would like to thank Adam Carter, formerly of HP LeftHand Networks; Chad Sakac of EMC; Vaughn Stewart of NetApp; and Andrew Gilman of Dell. All four individuals were invaluable in allowing me to bounce ideas around and to ask newbie-like questions—regarding not just their technologies, but storage issues in general. If I sound like some kind of storage guru in this book, I have these guys to thank for that. (Actually, I'm not a guru at all, even in terms of VMware products. I can't even stand the use of the word *guru*.) Within EMC, I would like to especially thank Alex Tanner, who is part of "Chad's Army" and was instrumental in getting me set up with the EMC NS-120 systems as well as giving me ongoing help and support as I rewrote the material in the previous edition for use in this edition of the book. I would also like to thank Luke Reed of NetApp who helped in a very similar capacity in updating my storage controllers so that I could use them with the latest version of ONTAP.

Third, I would like to thank Jacob Jenson of the VMware DR/BC Group and the SRM Team generally. I would also like to thank Mornay Van Der Walt of VMware. Mornay is the director for Enterprise & Technical Marketing. I first met Mornay at Cannes in 2008, and he was instrumental in introducing me to the right people when I first took on SRM as a technology. He was also very helpful in assisting me with my more obscure technical questions surrounding the early SRM product without which the idea of writing a book would have been impossible. I would also like to thank Lee Dilworth of VMware in the UK. Lee has been very helpful in my travels with SRM, and it's to him that I direct my emails when even I can't work out what is going on!

I would like to thank Cormac Hogan, Tim Oudin, Craig Waters, and Jeff Drury for their feedback. I'm often asked how much of a technical review books like mine go through. The answer is a great deal—and this review process is often as long as the writing process. People often offer to review my work, but almost never have the time to do it. So I would like to thank these guys for taking the time and giving me their valuable feedback.

*This page intentionally left blank*

## About the Author

**Mike Laverick** is a former VMware instructor with 17 years of experience in technologies such as Novell, Windows, Citrix, and VMware. He has also been involved with the VMware community since 2003. Laverick is a VMware forum moderator and member of the London VMware User Group. Laverick is the man behind the virtualization website and the blog RTFM Education, where he publishes free guides and utilities for VMware customers. Laverick received the VMware vExpert award in 2009, 2010, and 2011.

Since joining TechTarget as a contributor, Laverick has also found the time to run a weekly podcast called, alternately, the *Chinwag* and the *Vendorwag*. Laverick helped found the Irish and Scottish VMware user groups and now regularly speaks at larger regional events organized by the Global VMUG in North America, EMEA, and APAC. Laverick previously published several books on VMware Virtual Infrastructure 3, vSphere 4, Site Recovery Manager, and View.



*This page intentionally left blank*

## We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

As an associate publisher for Pearson, I welcome your comments. You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books better.

*Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.*

When you write, please be sure to include this book's title and author as well as your name, email address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: [VMwarePress@vmware.com](mailto:VMwarePress@vmware.com)

Mail: David Dusthimer  
Associate Publisher  
Pearson  
800 East 96th Street  
Indianapolis, IN 46240 USA

*This page intentionally left blank*

# Configuring the Protected Site

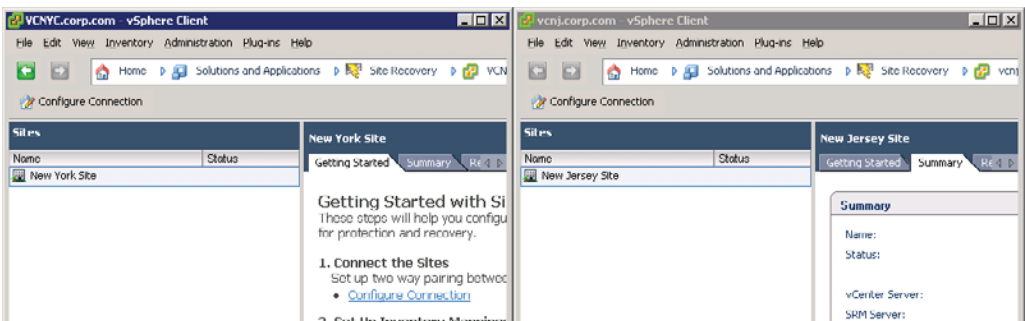
Now that the core SRM product is installed it's possible to progress through the post-configuration stages. Each of these stages depends highly on the previous configuration being completed correctly. It would be correct to assume that this then creates a dependency between each stage such that you must be careful about making changes once the components have been interlinked. Essentially, the post-configuration stages constitute a “workflow.” The first step is to pair the two sites together, which creates a relationship between the Protected Site (NYC) and the Recovery Site (NJ). Then we can create inventory mappings that enable the administrator to build relationships between the folders, resource pools, or clusters and networks between the Protected Site and the Recovery Site. These inventory mappings ensure that VMs are recovered to the correct location in the vCenter environment. At that point, it is possible to configure the array managers. At this stage you make the sites aware of the identities of your storage systems at both locations; the SRM will interrogate the arrays and discover which datastores have been marked for replication. The last two main stages are to create Protection Groups and to create Recovery Plans. You cannot create Recovery Plans without first creating Protection Groups, as their name implies the point to the datastores that you have configured for replication. The Protection Groups use the inventory mappings to determine the location of what VMware calls “placeholder VMs.” These placeholder VMs are used in Recovery Plans to indicate when and where they should be recovered and allows for advanced features such as VM Dependencies and scripting callouts. I will be going through each step in detail, walking you through the configuration all the way so that by the end of the chapter, you should really understand what each stage entails and why it must be completed.

## Connecting the Protected and Recovery Site SRMs

One of the main tasks carried out in the first configuration of SRM is to connect the Protected Site SRM to the Recovery Site SRM. It's at this point that you configure a relationship between the two, and really this is the first time you indicate which is the Protected Site and which is the Recovery Site. It's a convention that you start this pairing process at the Protected Site. The reality is that the pairing creates a two-way relationship between the locations anyway, and it really doesn't matter from which site you do this. But for my own sanity, I've always started the process from the protected location.

When doing this first configuration, I prefer to have two vSphere client windows open: one on the protected vCenter and the other on the recovery vCenter. This way, I get to monitor both parts of the pairing process. I did this often in my early use of SRM so that I could see in real time the effect of changes in the Protected Site on the Recovery Site. Of course, you can simplify things greatly by using the linked mode feature in vSphere. Although with SRM new views show both the Recovery and Protected Sites at the same time, the benefits of linked mode are somewhat limited; however, I think linked mode can be useful for your general administration. For the moment, I'm keeping the two vCenters separate so that it's 100% clear that one is the Protected Site and the other is the Recovery Site (see Figure 9.1).

As you might suspect, this pairing process clearly means the Protected Site SRM and Recovery Site SRM will need to communicate to each other to share information. It is possible to have the same IP range used at two different geographical locations. This networking concept is called "stretched VLANs." Stretched VLANs can greatly simplify the pairing process, as well as greatly simplify the networking of virtual machines when you run tests or invoke your Recovery Plans. If you have never heard of stretched VLANs, it's well worth brushing up on them, and considering their usage to facilitate DR/BC. The stretched VLAN configuration, as we will see later, can actually ease the administrative



**Figure 9.1** The Protected Site (New York) is on the left; the Recovery Site (New Jersey) is on the right.

burden when running test plans or invoking DR for real. Other methods of simplifying communications, especially when testing and running Recovery Plans, include the use of network address translation (NAT) systems or modifying the routing configuration between the two locations. This can stop the need to re-IP the virtual machines as they boot in the DR location. We will look at this in more detail in subsequent chapters.

This pairing process is sometimes referred to as “establishing reciprocity.” In the first release of SRM the pairing process was one-to-one, and it was not possible to create hub-and-spoke configurations where one site is paired to many sites. The structure of SRM 1.0 prevented many-to-many SRM pairing relationships. Back in SRM 4.0, VMware introduced support for a shared-site configuration where one DR location can provide resources for many Protected Sites. However, in these early stages I want to keep with the two-site configuration.

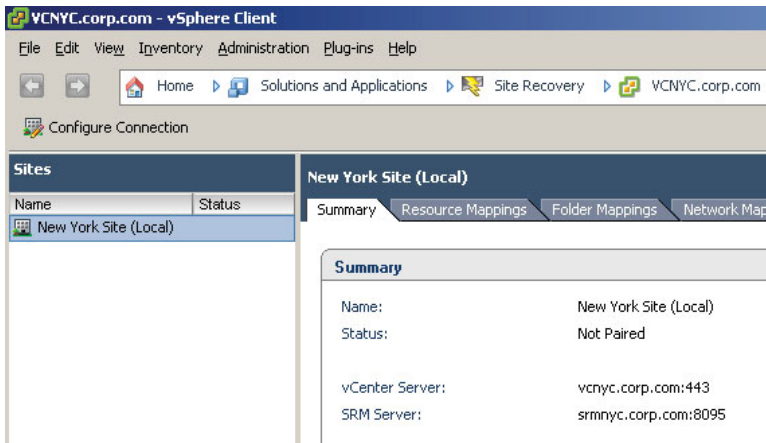
Installing the SRM and vCenter software on the same instance of Windows can save you a Windows license. However, some people might consider this approach as increasing their dependence on the management system of vCenter. If you like, there is a worry or anxiety about creating an “all-eggs-in-one-basket” scenario. If you follow this rationale to its logical extreme, your management server will have many jobs to do, such as being the

- vCenter server
- Web access server
- Converter server
- Update Manager server

My main point, really, is that if the pairing process fails, it probably has more to do with IP communication, DNS name resolution, and firewalls than anything else. IP visibility from the Protected to the Recovery Site is required to set up SRM. Personally, I always recommend dedicated Windows instances for the SRM role, and in these days of Microsoft licensing allowing multiple instances of Enterprise and Datacenter Editions on the same hypervisor, the cost savings are not as great as they once were.

When connecting the sites together you always log in to the Protected Site and connect it to the Recovery Site. This starting order dictates the relationship between the two SRM servers.

1. Log in with the vSphere client to the vCenter server for the Protected Site SRM (New York).
2. In the Sites pane, click the Configure Connection button shown in Figure 9.2. Alternatively, if you still have the Getting Started tab available, click the Configure Connection link.

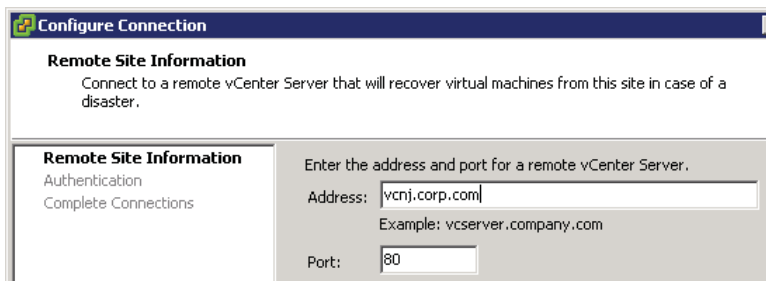


**Figure 9.2** The status of the New York Site is “not paired” until the Configure Connection Wizard is run.

Notice how the site is marked as being “local,” since we logged in to it directly as though we are physically located at the New York location. If I had logged in to the New Jersey site directly it would be earmarked as local instead.

3. In the Configure Connection dialog box enter the name of the vCenter for the Recovery Site, as shown in Figure 9.3.

When you enter the vCenter hostname use lowercase letters; the vCenter hostname must be entered exactly the same way during pairing as it was during installation (for example, either fully qualified in all cases or not fully qualified in all cases). Additionally, although you can use either a name or an IP address during the pairing process, be consistent. Don’t use a mix of IP addresses and FQDNs together, as



**Figure 9.3** Despite the use of port 80 in the dialog box, all communication is redirected to port 443.

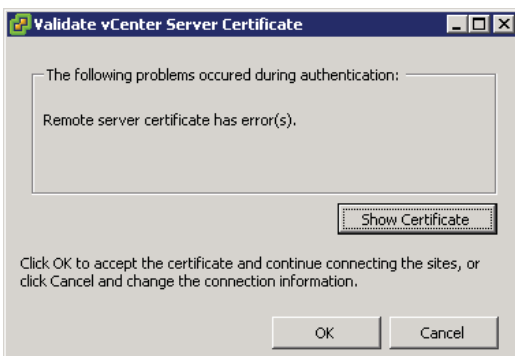
this only confuses SRM. As we saw earlier during the installation, despite entering port 80 to connect to the vCenter system, it does appear to be the case that communication is on port 443.

Again, if you are using the untrusted auto-generated certificates that come with a default installation of vCenter you will receive a certificate security warning dialog box, as shown in Figure 9.4. The statement “Remote server certificate has error(s)” is largely an indication that the certificate is auto-generated and untrusted. It doesn’t indicate fault in the certificate itself, but rather is more a reflection of its status.

4. Specify the username and password for the vCenter server at the Recovery Site.

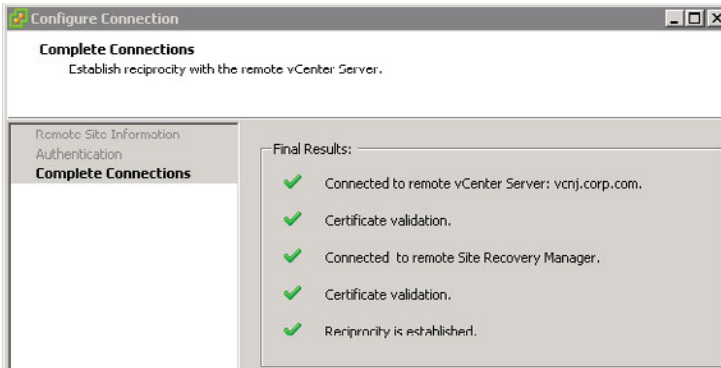
Again, if you are using the untrusted auto-generated certificates that come with a default installation of SRM you will receive a certificate security warning dialog box. This second certificate warning is to validate the SRM certificate, and is very similar to the previous dialog box for validating the vCenter certificate of the Recovery Site. So, although these two dialog boxes look similar, they are issuing warnings regarding completely different servers: the vCenter server and the SRM server of the Recovery Site. Authentication between sites can be difficult if the Protected and Recovery Sites are different domains and there is no trust relationship between them. In my case, I opted for a single domain that spanned both the Protected and Recovery Sites.

5. At this point the SRM wizard will attempt to pair the sites, and the Complete Connections dialog box will show you the progress of this task, as shown in Figure 9.5, on the Recent Tasks of the Protected vCenter.
6. At the end of the process you will be prompted to authenticate the vSphere client against the remote (Recovery) site. If you have two vSphere clients open at the same



**Figure 9.4** Dialog box indicating there is an error with the remote server certificate



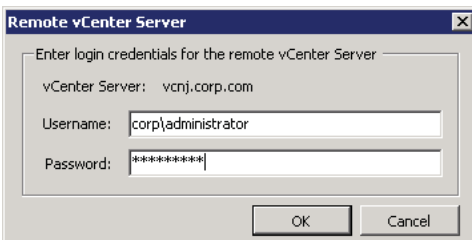


**Figure 9.5** Pairing the sites (a.k.a. establishing reciprocity)

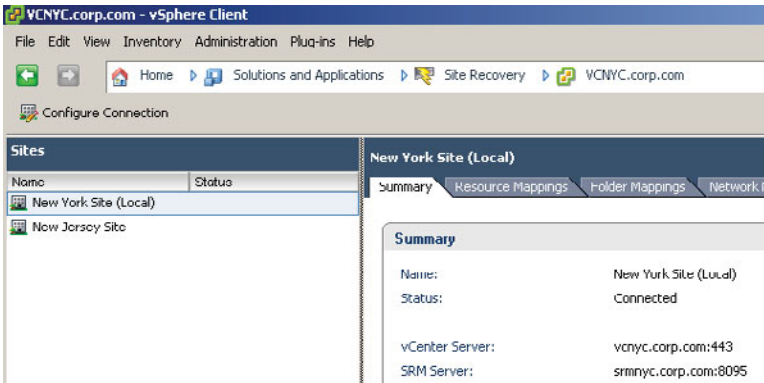
time on both the Protected and Recovery Sites you will receive two dialog login box prompts, one for each SRM server. Notice how in the dialog box shown in Figure 9.6 I'm using the full NT domain-style login of DOMAIN\Username. This dialog box appears each time you load the vSphere client and select the SRM icon.

At the end of this first stage you should check that the two sites are flagged as being connected for both the local site and the paired site, as shown in Figure 9.7.

Additionally, under the Commands pane on the right-hand side you will see that the Break Connection link is the reverse of the pairing process. It's hard to think of a use case for this option. But I guess you may at a later stage unpair two sites and create a different relationship. In an extreme case, if you had a real disaster the original Protected Site might be irretrievably lost. In this case, you would have no option but to seek a different site to maintain your DR planning. Also in the Commands pane you will find the option to export your system logs. These can be invaluable when it comes to troubleshooting, and you'll need them should you raise an SR with VMware Support. As you can see, SRM has a new interface, and even with vCenter linked mode available this new UI should reduce the amount of time you spend toggling between the Protected and Recovery Sites. Indeed, for



**Figure 9.6** Entering login credentials for the Recovery Site vCenter



**Figure 9.7** The sites are connected and paired together; notice how communication to the vCenter in the Recovery Site used port 443.

the most part I only keep my vCenters separated in this early stage when I am carrying out customer demonstrations; it helps to keep the customer clear on the two different locations.

From this point onward, whenever you load the vSphere client for the first time and click the Site Recovery Manager icon you will be prompted for a username and password for the remote vCenter. The same dialog box appears on the Recovery Site SRM. Although the vSphere client has the ability to pass through your user credentials from your domain logon, this currently is not supported for SRM, mainly because you could be using totally different credentials at the Recovery Site anyway. For most organizations this would be a standard practice—two different vCenters need two different administration stacks to prevent the breach of one vCenter leading to a breach of all others.

## Configuring Inventory Mappings

The next stage in the configuration is to configure inventory mappings. This involves mapping the resources (clusters and resource pools), folders, and networks of the Protected Site to the Recovery Site. Ostensibly, this happens because we have two separate vCenter installations that are not linked by a common data source. This is true despite the use of linked mode in vSphere. The only things that are shared between two or more vCenters in linked mode are licensing, roles, and the search functionality. The remainder of the vCenter metadata (datacenters, clusters, folders, and resource pools) is still locked inside the vCenter database driven by Microsoft SQL, Oracle, or IBM DB2.

When your Recovery Plan is invoked for testing or for real, the SRM server at the Recovery Site needs to know your preferences for bringing your replicated VMs online. Although the recovery location has the virtual machine files by virtue of third-party

replication software, the metadata that comprises the vCenter inventory is not replicated. It is up to the SRM administrator to decide how this “soft” vCenter data is handled. The SRM administrator needs to be able to indicate what resource pools, networks, and folders the replicated VMs will use. This means that when VMs are recovered they are brought online in the correct location and function correctly. Specifically, the important issue is network mappings. If you don’t get this right, the VMs that are powered on at the Recovery Site might not be accessible across the network.

Although this “global default” mapping process is optional, the reality is that you will use it. If you wish, you can manually map each individual VM to the appropriate resource pool, folder, and network when you create Protection Groups. The Inventory Mappings Wizard merely speeds up this process and allows you to set your default preferences. It is possible to do this for each virtual machine individually, but that is very administratively intensive. To have to manually configure each virtual machine to the network, folder, and resource pool it should use in the Recovery Site would be very burdensome in a location with even a few hundred virtual machines. Later in this book we will look at these per-virtual-machine inventory mappings as a way to deal with virtual machines that have unique settings. In a nutshell, think of inventory mappings as a way to deal with virtual machine settings as though they are groups and the other methods as though you were managing them as individual users.

It is perfectly acceptable for certain objects in the inventory mappings to have no mapping at all. After all, there may be resource pools, folders, and networks that do not need to be included in your Recovery Plan. So, some things do not need to be mapped to the Recovery Site, just like not every LUN/volume in the Protected Site needs replicating to the Recovery Site. For example, test and development virtual machines might not be replicated at all, and therefore the inventory objects that are used to manage them are not configured. Similarly, you may have “local” virtual machines that do not need to be configured; a good example might be that your vCenter and its SQL instance may be virtualized. By definition, these “infrastructure” virtual machines are not replicated at the Recovery Site because you already have duplicates of them there; that’s part of the architecture of SRM, after all. Other “local” or site-specific services may include such systems as anti-virus, DNS, DHCP, Proxy, Print, and, depending on your directory services structure, Active Directory domain controllers. Lastly, you may have virtual machines that provide deployment services—in my case, the UDA—that do not need to be replicated at the Recovery Site as they are not business-critical, although I think you would need to consider how dependent you are on these ancillary virtual machines for your day-to-day operations. In previous releases, such objects that were not included in the inventory mapping would have the label “None Selected” to indicate that no mapping had been configured. In this new release, VMware has dispensed with this label. Remember, at this stage we are not indicating which VMs will be included in our recovery procedure. This is done at a later stage when we create SRM Protection Groups. Let me remind you (again) of my folder, resource pool, and network structures (see Figure 9.8, Figure 9.9, and Figure 9.10).

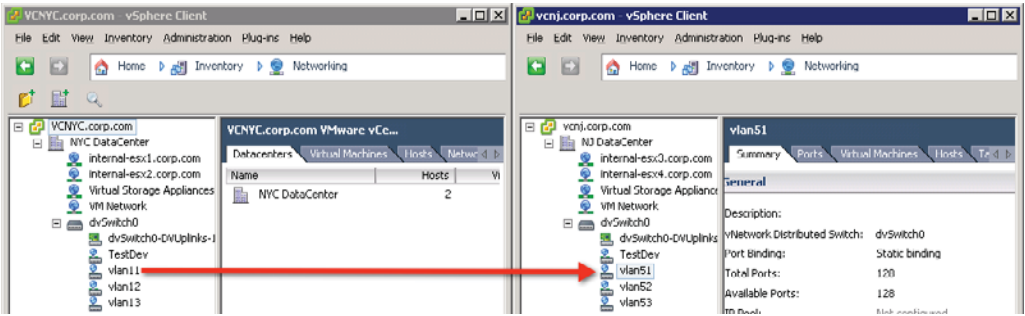


Figure 9.8 My vSwitch configuration at the Protected and Recovery Sites

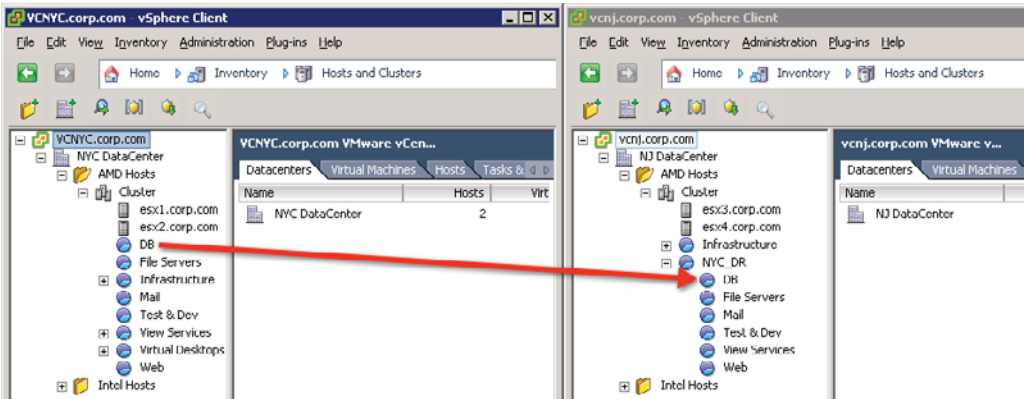


Figure 9.9 My resource pool configuration at the Protected and Recovery Sites

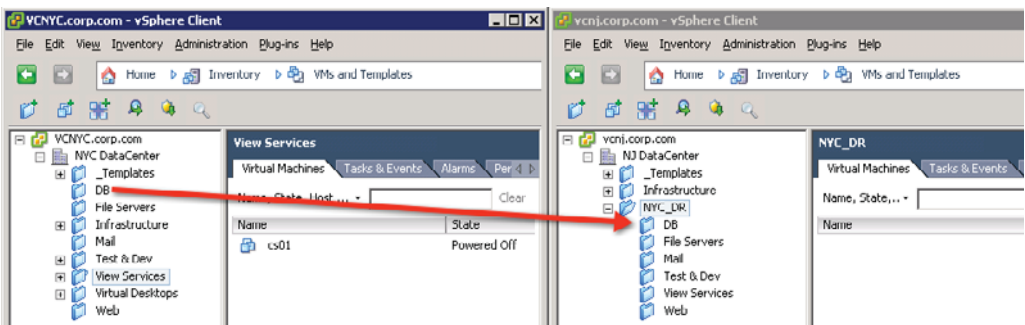


Figure 9.10 My VM folder configuration at the Protected and Recovery Sites

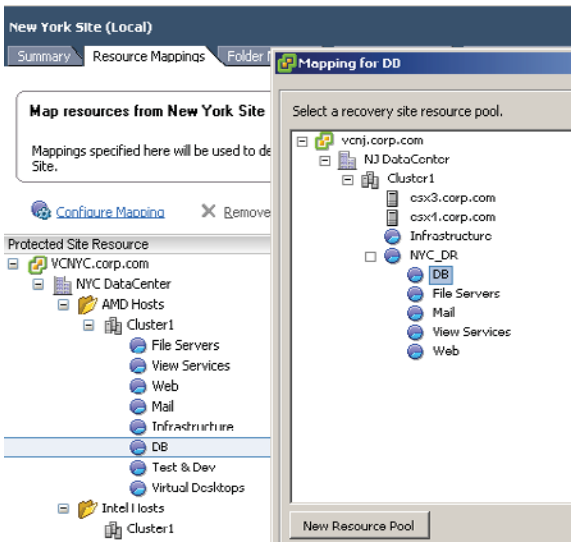
The arrows represent how I will be “mapping” these resources from the Protected Site to the Recovery Site. SRM uses the term *resource mapping* to refer to clusters of ESX hosts and the resource pools within.

Finally, it’s worth mentioning that these inventory mappings are used during the reprotect and failback processes. After all, if VMs have been failed over to specific folders, resource pools, and networks, when a failback occurs, those VMs must be returned to their original locations at the Protected Site. No special configuration is required to achieve this—the same inventory mappings used to move VMs from the Protected to the Recovery Site are used when the direction is reversed.

## Configuring Resource Mappings

To configure resource mappings, follow these steps.

1. Log on with the vSphere client to the Protected Site’s vCenter.
2. Click the Site Recovery icon.
3. Select the Protected Site (in my case, this is New York), and then select the Resource Mapping tab.
4. Double-click your resource pool or the cluster you wish to map, or click the Configure Mapping link as shown in Figure 9.11.



**Figure 9.11** In the foreground is the Mapping for DB dialog box where the resource pool in New York is mapped to the NYC\_DR\DB resource pool in New Jersey.

Notice how the “Mapping for...” dialog box also now includes the new option to create a new resource pool if it’s needed. Remember that the use of resource pools is by no means mandatory. You can run all your VMs from the DRS-enabled cluster, if you prefer. Once you understand the principle of inventory mappings this becomes a somewhat tedious but important task of mapping the correct Protected Site vCenter objects to the Recovery Site vCenter objects.

## Configuring Folder Mappings

In my early days of using SRM, I used to take all the VMs from the Protected Site and dump them into one folder called “Recovery VMs” on the Recovery Site’s vCenter. I soon discovered how limiting this would be in a failback scenario. I recommend more or less duplicating the folder and resource pool structure at the Recovery Site, so it exactly matches the Protected Site. This offers more control and flexibility, especially when you begin the failback process. I would avoid the casual and cavalier attitude of dumping virtual machines into a flat-level folder.

As you can see in Figure 9.12, I have not bothered to map every folder in the Protected Site to every other folder in the Recovery Site. I’ve decided I will never be using SRM to failover and failback VMs in the Infrastructure or Test & Dev VM folder. There’s little point in creating a mapping if I have no intention of using SRM with these particular VMs.

The screenshot shows the SRM console for the New York Site (Local). The 'Folder Mappings' tab is active, displaying a table of mappings between the Protected Site Resource and the Recovery Site Resource. The table lists various folders and resource pools, such as DB, File Servers, Infrastructure, Mail, Test & Dev, View Services, Virtual Desktops, and Web, along with their corresponding paths in the Recovery Site. A note at the top states: 'Map folders from New York Site (Local) to folders at New Jersey Site. Mappings specified here will be used to determine the location for protected virtual machines when they are recovered to New Jersey Site.'

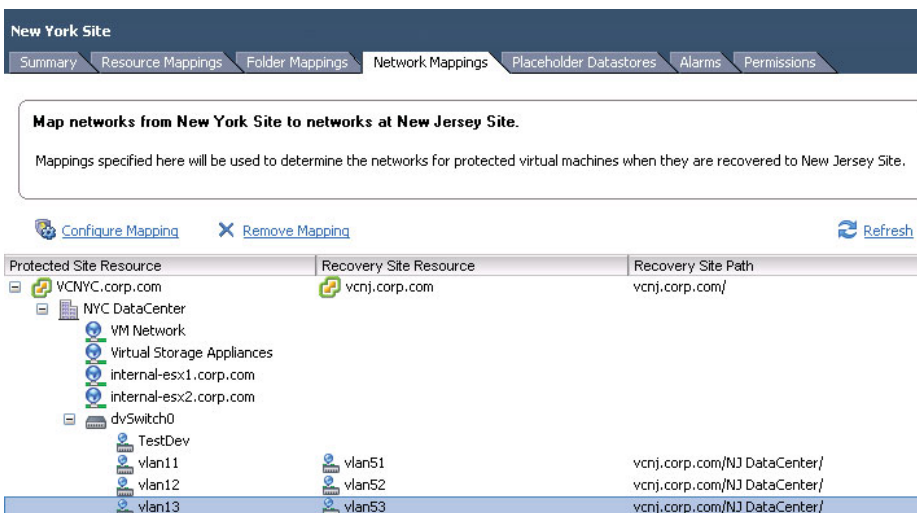
Protected Site Resource	Recovery Site Resource	Recovery Site Path
VCWNC.corp.com	vcnj.corp.com	vcnj.corp.com/
NYC DataCenter		
DB	DB	vcnj.corp.com/NJ DataCenter/NYC_DR/
File Servers	File Servers	vcnj.corp.com/NJ DataCenter/NYC_DR/
Infrastructure		
Mail	Mail	vcnj.corp.com/NJ DataCenter/NYC_DR/
Test & Dev		
View Services	View Services	vcnj.corp.com/NJ DataCenter/NYC_DR/
Virtual Desktops		
Web	Web	vcnj.corp.com/NJ DataCenter/NYC_DR/
_Templates		

**Figure 9.12** My folder inventory mappings. Only the folders and resource pools that SRM will need in order to protect the VMs must be mapped.

## Configuring Network Mappings

By default, when you run a test Recovery Plan the Recovery Site SRM will auto-magically put the replicated VMs into a bubble network which isolates them from the wider network using an internal vSwitch. This prevents possible IP and NetBIOS in Windows conflicts. Try to think of this bubble network as a safety valve that allows you to test plans with a guarantee that you will generate no conflicts between the Protected Site and the Recovery Site. So, by default, these network settings are only used in the event of triggering your Recovery Plan for real. If I mapped this “production” network to the “internal” switch, no users would be able to connect to the recovered VMs. Notice in Figure 9.13 how I am not mapping the VM Network or Virtual Storage Appliance port group to the Recovery Site. This is because the VMs that reside on that network deliver local infrastructure resources that I do not intend to include in my Recovery Plan.

Networking and DR can be more involved than you first think, and much depends on how you have the network set up. When you start powering on VMs at the Recovery Site they may be on totally different networks requiring different IP addresses and DNS updates to allow for user connectivity. The good news is that SRM can control and automate this process. One very easy way to simplify this for SRM is to implement stretched VLANs where two geographically different locations appear to be on the same VLAN/subnet. However, you may not have the authority to implement this, and unless it is already in place it is a major change to your physical switch configuration, to say the least. It’s worth making it clear that even if you do implement stretched VLANs you may still have to create inventory mappings because of port group differences. For example, there may be a VLAN



**Figure 9.13** Map only the port groups that you plan to use in your Recovery Plan.

**New York Site (Local)**

Summary Resource Mappings Folder Mappings **Network Mappings** Placeholder Datastores Alarms Permissions

**Map networks from New York Site (Local) to networks at New Jersey Site.**

Mappings specified here will be used to determine the networks for protected virtual machines when they are recovered to New Jersey Site.

Configure Mapping Remove Mapping Refresh

Protected Site Resource	Recovery Site Resource	Recovery Site Path
VCNYC.corp.com	vcnj.corp.com	vcnj.corp.com/
<ul style="list-style-type: none"> <li>NYC DataCenter           <ul style="list-style-type: none"> <li>VM Network</li> <li>Virtual Storage Appliances</li> <li>internal-esx1.corp.com</li> <li>internal-esx2.corp.com</li> <li>dvSwitch0               <ul style="list-style-type: none"> <li>vlan11</li> <li>vlan12</li> <li>vlan13</li> </ul> </li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>vlan51</li> <li>vlan52</li> <li>vlan53</li> </ul>	<ul style="list-style-type: none"> <li>vcnj.corp.com/NJ DataCenter/</li> <li>vcnj.corp.com/NJ DataCenter/</li> <li>vcnj.corp.com/NJ DataCenter/</li> </ul>

**Figure 9.14** Network mappings can include different switch types if needed.

101 in New York and a VLAN 101 in New Jersey. But if the administrative team in New York calls their port groups on a virtual switch “NYC-101” and the guys in Chicago call theirs “NJ-101” you would still need a port group mapping in the Inventory Mappings tab.

Finally, in my experience it is possible to map between the two virtual switch types of Distributed and Standard vSwitches (see Figure 9.14). This does allow you to run a lower-level SKU of the vSphere 5 product in the DR location. So you could be using Enterprise Plus in the Protected Site and the Advanced version of vSphere 5 in the Recovery Site. People might be tempted to do this to save money on licensing. However, I think it is fraught with unexpected consequences, and I do not recommend it; it’s a recipe for negative unforeseen outcomes. For example, an eight-way VM licensed for Enterprise Plus in the Protected Site would not start in the Recovery Site. A version of vSphere 5 that doesn’t support DRS clustering and the initial placement feature would mean having to map specific VMs to specific ESX hosts. So you certainly can map DvSwitches to SvSwitches, and vice versa. To SRM, port groups are just labels and it just doesn’t care. But remember, if VM is mapped from a DvSwitch to the SvSwitch it may lose functionality that only the DvSwitch can provide.

## Assigning Placeholder Datastores

As we will see later in this chapter, an important part of the wizard for creating Protection Groups is selecting a destination for placeholders for the Recovery Site. This is a VMFS



or NFS volume at the recovery location. When you create a Protection Group at the production site, SRM creates a VMX file and the other smaller files that make up the virtual machine from the Protected Site to the Recovery Site using the placeholder datastore selected in the wizard. It then preregisters these placeholder VMX files to the ESX host at the Recovery Site. This registration process also allocates the virtual machine to the default resource pool, network, and folder as set in the inventory mappings section. Remember, your real virtual machines are really being replicated to a LUN/volume on the storage array at the Recovery Site. You can treat these placeholders as an ancillary VM used just to complete the registration process required to get the virtual machine listed in the Recovery Site's vCenter inventory. Without the placeholder VMs, there would be no object to select when you create Recovery Plans.

If you think about it, although we are replicating our virtual machines from the Protected Site to the Recovery Site, the VMX file does contain site-specific information, especially in terms of networking. The VLAN and IP address used at the recovery location could differ markedly from the protected location. If we just used the VMX as it was in the replicated volume, some of its settings would be invalid (port group name and VLAN, for example), but others would not change (amount of memory and CPUs).

The main purpose of placeholder VMX files is that they help you see visually in the vCenter inventory where your virtual machines will reside prior to executing the Recovery Plan. This allows you to confirm up front whether your inventory mappings are correct. If a virtual machine does not appear at the Recovery Site, it's a clear indication that it is not protected. It would have been possible for VMware to create the virtual machine at the Recovery Site at the point of testing the Recovery Plan, but doing it this way gives the operator an opportunity to fix problems before even testing a Recovery Plan.

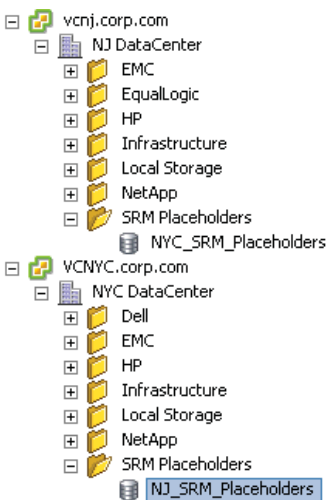
So, before you begin configuring the array manager of Protection Groups, you should create a small, 5–10GB volume on the storage array of your choice and present that to all the ESX hosts that will perform DR functions. For example, on my EMC NS-120 array I created a 5GB LUN visible to my Recovery Site ESX hosts (esx3/4), called using EMC's Virtual Storage Console formatted with VMFS, and giving it a friendly volume name of SRM\_Placeholders. It's a good practice to keep the placeholder datastores relatively small, distinct, and well named to stop people from storing real VMs on them. If you wish, you could use datastore folders together with permissions to stop this from happening.

It's worth stating that if you ever want to run your Recovery Plan (failover) for real, either for planned migration or for disaster recovery, you would need a placeholder datastore at the Protected Site as well for returning to the production location as part of any reprotect and automated failback procedure. This has important consequences if you want to easily use the new automatic failback process or reprotect features. I'd go so far as to say that you might as well create a placeholder volume at both locations at the very beginning.

This placeholder datastore needs to be presented to every ESX host in the cluster that would act as a recovery host in the event of DR. The datastore could be used across clusters if you so wished, so long as it was presented to all the hosts that need to have access to it in the site. For me, each cluster represents an allocation of memory, CPU, network, *and* storage. In my case, I created placeholder datastores at New Jersey used in the process of protecting VMs in New York, and similarly I created placeholder datastores at New York used in the process of protecting VMs in New Jersey. In most cases you will really need only one placeholder datastore per cluster. As I knew at some stage I would need to do a failover and failback process in SRM it made sense to set these placeholder datastores at this stage, as shown in Figure 9.15.

Remember, the smallest VMFS volume you can create is 1.2GB. If the volume is any smaller than this you will not be able to format it. The placeholder files do not consume much space, so small volumes should be sufficient, although you may wish to leverage your storage vendor's thin-provisioning features so that you don't unnecessarily waste space—but hey, what's a couple of gigabytes in the grand scheme of things compared to the storage footprint of the VMs themselves? On NFS you may be able to have a smaller size for your placeholder datastore; much depends on the array—for example, the smallest volume size on my NetApp FAS2040 is 20GB.

It really doesn't matter what type of datastore you select for the placeholder VMX file. You can even use local storage; remember, only temporary files are used in the SRM

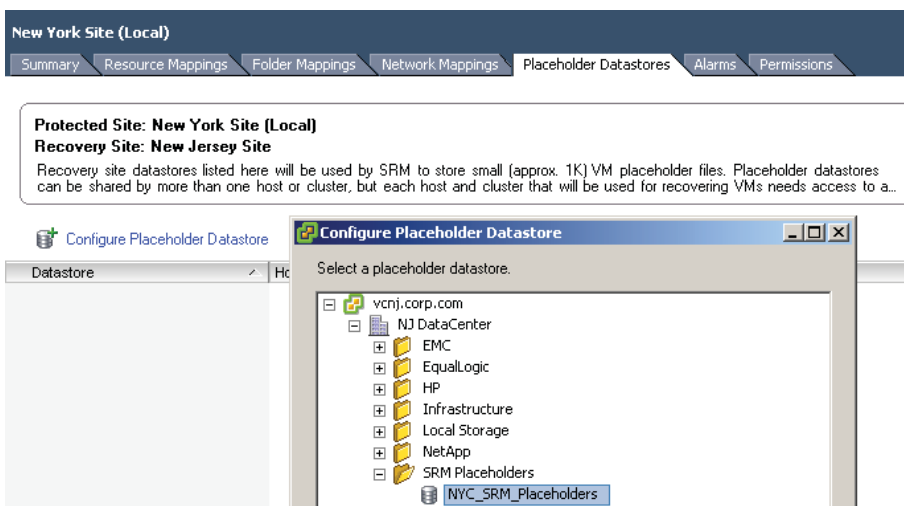


**Figure 9.15** Placeholder datastores should be on nonreplicated datastores available to all hosts in the datacenter or clusters where SRM is in use.

process. However, local storage is perhaps not a very wise choice. If that ESX host goes down, is in maintenance mode, or is in a disconnected state, SRM would not be able to access the placeholder files while executing a Recovery Plan. It would be much better to use storage that is shared among the ESX hosts in the Recovery Site. If one of your ESX hosts was unable to access the shared storage location for placeholder files, it would merely be skipped, and no placeholder VMs would be registered on it. The size of the datastore does not have to be large; the placeholder files are the smaller files that make up a virtual machine, they do not contain virtual disks.

But you might find it useful to either remember where they are located, or set up a dedicated place to store them, rather than mixing them up with real virtual machine files. It is a good practice to use folder and resource pool names that reflect that these placeholder virtual machines are not “real.” In my case, the parent folder and resource pool are called “NYC\_DR” at the New Jersey Recovery Site. Once the placeholder datastore has been created, you can configure SRM at the Protected Site and use it to create the “shadow” VMs in the inventory.

1. In SRM, select the Protected Site; in my case, this is the New York site.
2. Select the Placeholder Datastores tab (see Figure 9.16).
3. Click the Configure Placeholder Datastore link.
4. In the subsequent dialog box, select the datastore(s) you created.



**Figure 9.16** The Placeholder Datastores tab

The dialog box in Figure 9.16 does allow you to add multiple placeholder datastores for each cluster that you have. The choice is yours: one placeholder datastore for *all* your clusters, or one placeholder datastore for each cluster in vCenter. Your choice will very much depend on your storage layer and policies within your organization. For example, if you are using IP-based storage it will be very easy to present an iSCSI or NFS volume across many VMware clusters. If you're using Fibre Channel, this could involve some serious work with zoning and masking at the switch and storage management layer. It may be your storage team's policy that each ESX host in a VMware cluster represents a block of storage or a "pod" that cannot be presented to other hosts outside the cluster.

If you look closely at the screen grab you can see that from New York Site (Local), I am browsing the datastores in the New Jersey vCenter. From there I can locate the datastore I called "NYC\_SRM\_Placeholders" as the location for the placeholder files. I configured a similar setup at the New Jersey location to facilitate the new automatic failback and reprotect features in SRM.

## Configuring Array Managers: An Introduction

The next essential part of SRM post-configuration involves enabling the array manager's piece of the product. The array manager is often just a graphical front end for supplying variables to the SRA. Of course I'm assuming you have a storage array which is supported for use with SRM. It may be that you don't, and you would prefer to use VMware's vSphere Replication (VR) instead.

If you do you have a storage array, it's in the Array Manager pane that you inform SRM what engine you are using to replicate your virtual machines from the Protected to the Recovery Site. In this process, SRA interrogates the array to discover which LUNs are being replicated, and enables the Recovery Site SRM to "mirror" your virtual machines to the recovery array. You must configure each array at the Protected Site that will take part in the replication of virtual machines. If a new array is added at a later stage it must be configured here. The array manager will not show every LUN/volume replicated on the storage array—just the ones used by your ESX hosts. The SRA works this out by looking at the files that make up the VM and only reporting LUNs/volumes which are in use by VMs on ESX hosts. This is why it's useful once you have set up the replication part of the puzzle to populate LUNs/volumes with VMs.

Clearly, the configuration of each array manager will vary from one vendor to the next. As much as I would like to be vendor-neutral at all times, it's not possible for me to validate every array manager configuration because that would be cost- and time-prohibitive.

However, if you look closely at the screen grabs for each SRA that I've included in this book you can see that they all share two main points. First, you must provide an IP address or URL to communicate with the storage array, and second, you must provide user credentials to authenticate with it. Most SRAs will have two fields for two IP addresses; this is usually for the first and second storage controllers which offer redundant connections into the array, whether it is based on Fibre Channel, iSCSI, or NFS. Sometimes you will be asked to provide a single IP address because your storage vendor has assumed that you have teamed your NIC interfaces together for load balancing and network redundancy. Different vendors label these storage controllers differently, so if you're familiar with NetApp perhaps the term *storage heads* is what you are used to, or if it's EMC CLARiiON you use the term *storage processor*. Clearly, for the SRA to work there must be a configured IP address for these storage controllers and it must be accessible to the SRM server.

As I stated in Chapter 7, Installing VMware SRM, there is no need now to restart the core SRM service (`vmware-dr`) when you install or upgrade an SRA. Of course, your environment can and will change over time, and there is room for mistakes. Perhaps, for instance, in your haste you installed the SRA into the Protected Site SRM server, but forgot to perform the same task at the Recovery Site. For this reason, VMware has added a Reload SRAs link, shown in Figure 9.17, under the SRAs tab in the Array Manager pane. If you do install or update an SRA it's worth clicking this button to make sure the system has the latest information.

Before beginning with the array manager configuration, it is worthwhile to check if there are any warnings or alerts in either the Summary tab or the SRAs tab, as this can prevent you from wasting time trying to configure the feature where it would never be successful. For example, if there is a mismatch between the SRAs installed at either the Protected or the Recovery Site you would receive a warning status on the affected SRA, as shown in Figure 9.18. This information displayed in the SRAs tab of the affected system can also tell you information about supported arrays and firmware.

Similarly, if your SRA has specific post-configuration requirements, and you subsequently fail to complete them, this can cause another status error message. For example, the message "The server fault 'DrStorageFaultCannotLoadAdapter'" was caused by my installation of the IMB SystemStorage SRA and not completing the configuration with the



**Figure 9.17** With the Reload SRAs link, the SRM administrator doesn't have to restart the core `vmware-dr` service for changes to take effect.

New York Site (Local)

Summary SRAs Permissions

[How do I download an approved Storage Replication Adapter \(SRA\)?](#) [Reload SRAs](#)

**SRA Errors**

⚠ The server fault 'DrStorageFaultCannotLoadAdapter' had no message.

**Acer Storage Replication Adapter for VMware vCenter SRM**

SRA:	Acer Storage Replication Adapter for VMware vCenter SRM
Status:	⚠ SRA not installed at the paired site
Version:	5.00 (Build 5010)
Vendor:	Acer, Inc.
Install location:	C:/Program Files (x86)/VMware/VMware vCenter Site Recovery Manager/storage/sra/Acer
Vendor URL:	
Supported array models:	Acer, Inc., Altos R720
Supported software:	ASC 5.0+

**Figure 9.18** To avoid false alarms, ensure that the SRA is installed on all the SRM servers before reloading the SRAs.

IBMSVCRAutil.exe program. The moral of the story is to not unnecessarily install SRAs that you don't need. I did because I'm a curious fellow; however, that curiosity often leads to learning something new that I can pass on to my customers and colleagues.

Most SRAs work the same way: You supply IP information and user authentication details to the wizard. By supplying to the Protected and Recovery Sites details regarding both IP address and authentication, you allow SRM to automate processes that would normally require the interaction of the storage management team or interaction with the storage management system. This is used specifically in SRM when a Recovery Plan is tested as the ESX host's HBAs in the recovery location are rescanned, and the SRA from the storage vendor allows them access to the replicated LUNs/volumes to allow the test to proceed. However, this functionality does vary from one storage array vendor to another. For example, these privileges in some arrays would allow for the dynamic creation and destruction of temporary snapshots, as is the case with EMC Celerra or NetApp filers. With other vendors someone on the storage team would have to grant access to the LUN and snapshot for this to be successful, as is the case with the EMC CLARiiON.

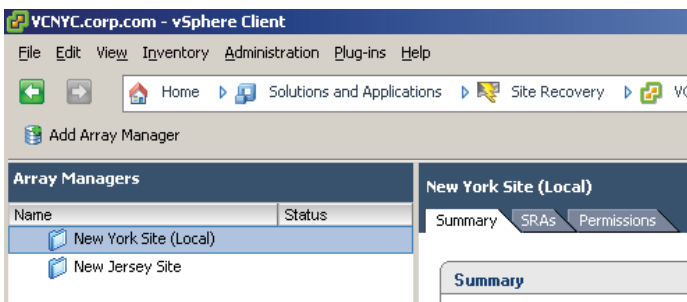
You might think that allowing this level of access to the storage layer would be deeply political; indeed, it could well be. However, in my discussions with VMware and those people who were among the first to try out SRM, this hasn't always been the case. In fact, many storage teams are more than happy to give up this control if it means fewer requests for manual intervention from the server or virtualization teams. You see, many storage

guys get understandably irritated if people like us are forever ringing them up to ask them to carry out mundane tasks such as creating a snapshot and then presenting it to a number of ESX hosts. The fact that we as SRM administrators can do that safely and automatically without their help takes this burden away from the storage team so that they can have time for other tasks. Unfortunately, for some companies this still might be a difficult pill for the storage team to swallow without fully explaining this to them before the remit of SRA. If there has been any annoyance for the storage team it has often been in the poor and hard-to-find documentation from the storage vendors. That has left some SRM administrators and storage teams struggling to work out the requirements to make the vendor's SRA function correctly.

Anyway, what follows is a blow-by-blow description of how to configure the array manager for the main storage vendors. If I were you, I would skip to the section heading that relates to the specific array vendor that you are configuring, because as I've said before, one array manager wizard is very similar to another. Array manager configuration starts with the same process, regardless of the array vendor.

1. Log on with the vSphere client to the Protected Site's vCenter—in my case, this is `vcnyc.corp.com`.
2. Click the Site Recovery icon.
3. Click the Array Managers icon.
4. Click the Add Array Manager button, as shown in Figure 9.19.

Once the array manager configuration has been completed and enabled, you will see in the Recent Tasks pane that it carries out four main tasks for each vCenter that is affected (see Figure 9.20).



**Figure 9.19** The Add Array Manager button that allows you to input your configuration specific to your SRA

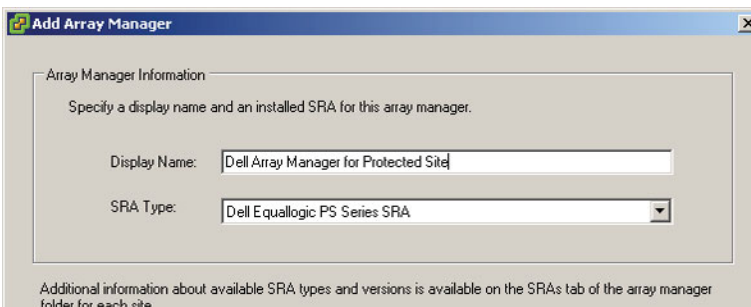
Recent Tasks		
Name	Target	Status
Recompute Datastore Groups	vcnj.corp.com	Completed
Recompute Datastore Groups	VCNYC.corp.com	Completed
Discover Replicated Devices	vcnj.corp.com	Completed
Discover Replicated Devices	VCNYC.corp.com	Completed
Add Array Pair	vcnj.corp.com	Completed
Add Array Pair	VCNYC.corp.com	Completed
Create Array Manager	vcnj.corp.com	Completed
Create Array Manager	VCNYC.corp.com	Completed

**Figure 9.20** Updating the array manager configuration or refreshing it will trigger events at both the Protected and Recovery Sites.

## Configuring Array Managers: Dell EqualLogic

To configure the array manager for the Dell EqualLogic, resume with these steps.

5. In the Add Array Manager dialog box, enter a friendly name for this manager, such as “Dell Array Manager for Protected Site”.
6. Select Dell EqualLogic PS Series SRA as the SRA Type, as shown in Figure 9.21.
7. Enter the IP address of the group at the Protected Site in the IP Address field; in my case, this is my New York EqualLogic system with the IP address of 172.168.3.69.
8. Supply the username and password for the Dell EqualLogic Group Manager.
9. Complete this configuration for the Partner Group; in my case, this is 172.168.4.69, the IP address of the Group Manager in New Jersey, as shown in Figure 9.22.



**Figure 9.21** Dell uses the concept of groups as collections of array members. You may wish to use a naming convention reflecting these group names.



**Add Array Manager**

Dell EqualLogic PS Series SRA

Managed Group

Local Group connection parameters

Group IP Address:   
Enter IP address of the Group

Username:   
Enter Username for Group

Password:   
Enter Password for Group

Partner Group

Partner Group Replication Parameters

Partner IP Address:   
Enter Partner Group IP Address

Username:   
Enter Partner Group Replication Username

Password:   
Enter Partner Group Replication Password

**Figure 9.22** Configuration of the Protected Site (local group connection parameters) and Recovery Site (partner group replication parameters)

These dialog boxes occasionally require you to scroll down in order to see all the fields.

10. Click Next and then Finish. Once the array manager configuration for the Protected Site is added, it should also add the array manager configuration for the Recovery Site, as shown in Figure 9.23.

The next step is to enable the configuration. If you have used SRM before you will recognize this is a new step in the array manager configuration. It’s designed to give the SRM administrator more control over the array pairs than was previously

Array Managers	
Name	Status
▼  New York Site (Local)	
Dell Array Manager for Protected Site	
▼  New Jersey Site	
Dell Array Manager for Recovery Site	

**Figure 9.23** The array manager configuration for both sites. You may want to use a naming convention reflecting the Dell EqualLogic group names.

possible. If you do not enable the pairing you will be unable to successfully create Protection Groups.

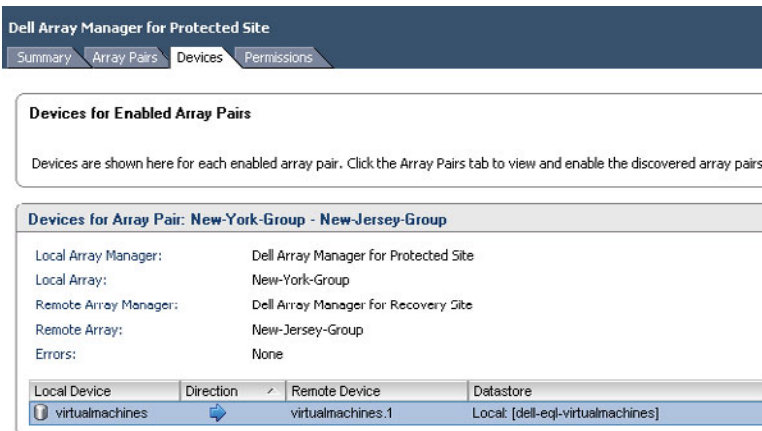
11. To enable the configuration select the Array Pairs tab on the array configuration object and click the Enable link under the Actions column (see Figure 9.24).

Occasionally, I've had to click Enable twice. This appears to be an issue with the way SRM refreshes this page. Once the array manager configuration is in use by Protection Groups it cannot be disabled. Similarly, once a Protection Group is being used by a Recovery Plan it cannot be removed until it is not referenced in a Recovery Plan.

This will complete the Remote Array Manager column with the name of the array configuration for the Recovery Site. If you look under the Devices tab you should see the volumes you are replicating to the Recovery Site. Notice in Figure 9.25 how the device or volume is local to the New York Site. Also notice how the blue arrow indicates the volume is being replicated to the remote location of New Jersey. This arrow changes direction



**Figure 9.24** Enabling the configuration of the Dell EqualLogic



**Figure 9.25** SRM's new interface shows the replication direction, and is useful when monitoring failover and failback procedures.

when you carry out an automated failback process, with the Reprotect button inverting the replication direction.

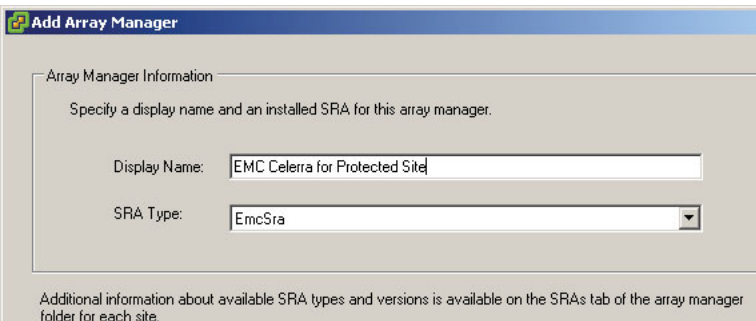
## Configuring Array Managers: EMC Celerra

EMC has one SRA that covers both the Unisphere range of arrays and the newer VMX series of systems together with “enabler” software for particular types of replication. So, regardless of the generation you possess, you should be able to install and configure it. Installing the EMC SRA VNX Replicator is a relatively simple affair. In this section, I will walk you through the configuration of the EMC Celerra with VMware SRM.

With EMC Celerra systems the SRM server will communicate to the Celerra at the Protected Site (New York) to collect volume information. It’s therefore necessary to configure a valid IP address for the SRM to allow this to occur *or* allow routing/intra-VLAN communication if your SRM and VSA reside on different networks. This is one of the challenges of installing your SRM and vCenter on the same instance of Windows. Another workaround is to give your SRM two network cards: one used for general communication and the other used specifically for communication to the Celerra. If you have no communication between the SRA and the Celerra you will receive an error message. Before you begin it’s a good idea to confirm that you can ping both the Protected Site array and the Recovery Site array with the Celerra Control Station IP from the Protected Site (New York) SRM server.

To configure the array manager for the EMC Celerra, resume with these steps.

5. In the Add Array Manager dialog box, enter a friendly name for this manager, such as “EMC Celerra for Protected Site”.
6. Select EmcSra as the SRA Type (see Figure 9.26).



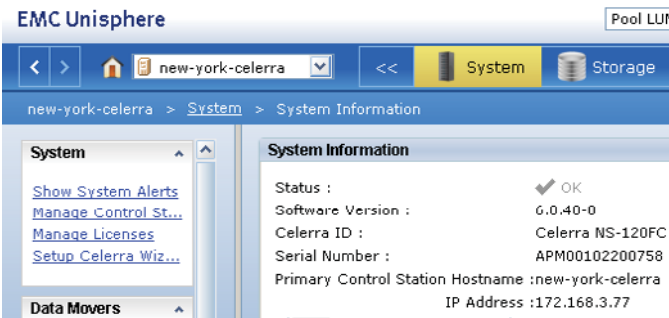
**Figure 9.26** If you have many Celerra systems you may want to develop a naming convention that allows you to uniquely identify them.

7. Enter the IP address of the Control Station at the Protected Site in the IP Address field—in my case, this is my New York Celerra system with the IP address of 172.168.3.77.

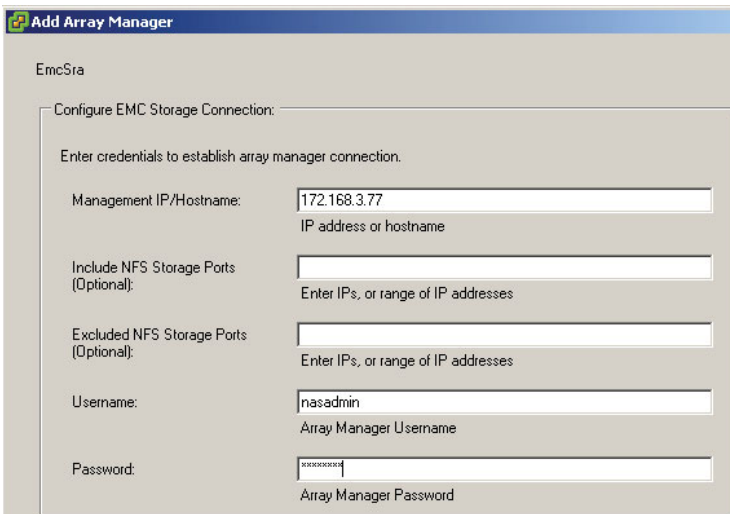
If you are unsure of the IP address of the Control Station for your system, you can locate it in the Unisphere management pages under System Information, as shown in Figure 9.27.

8. Supply the username and password for the Control Station (see Figure 9.28).

These dialog boxes occasionally require you to scroll down in order to see all the fields.



**Figure 9.27** Selecting the Celerra from the pull-down list and clicking the System button will show you the Control Station IP address.



**Figure 9.28** If you have NFS mount points as well as iSCSI these may be listening on different IP ports.

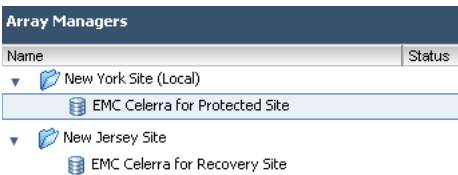
9. Click Next and then Finish. Once the array manager configuration for the Protected Site is added, you should also add the array manager configuration for the Recovery Site, as shown in Figure 9.29.

The next step is to enable the configuration, as shown in Figure 9.30. If you have used SRM before you will recognize this is a new step in the array manager configuration. It's designed to give the SRM administrator more control over the array pairs than was previously possible. If you do not enable the pairing you will be unable to successfully create Protection Groups.

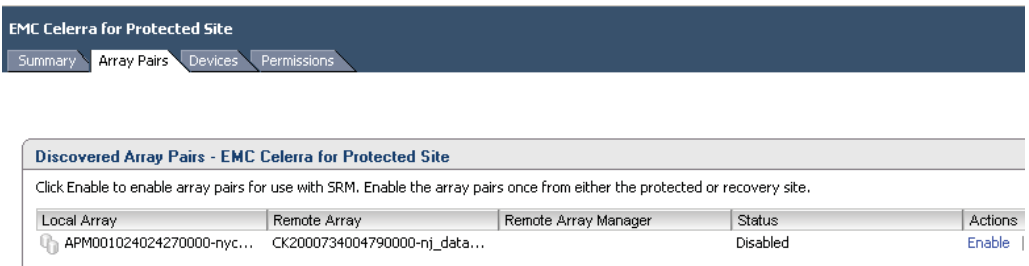
10. To enable the configuration select the Array Pairs tab on the array configuration object and click the Enable link under the Actions column.

Occasionally, I've had to click Enable twice. This appears to be an issue with the way SRM refreshes this page. Once the array manager configuration is in use by Protection Groups it cannot be disabled.

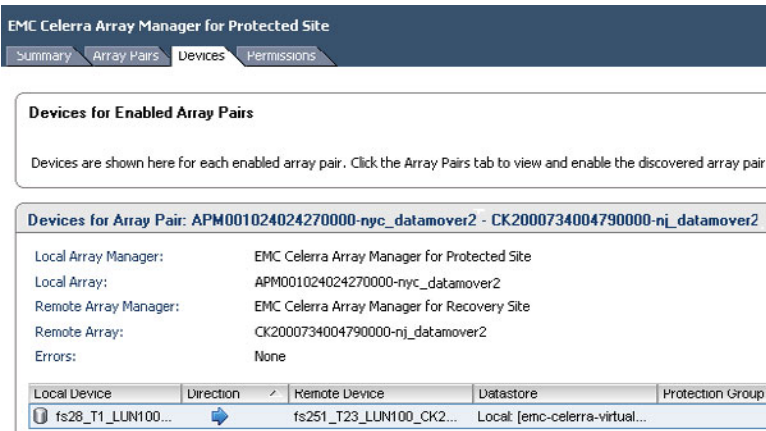
This will complete the Remote Array Manager column with the name of the array configuration for the Recovery Site. If you look under the Devices tab you should see the volumes you are replicating to the Recovery Site. Notice how the device or volume is local to the New York Site. Also notice how the blue arrow indicates the volume is being replicated to the remote location of New Jersey. This arrow changes direction when you carry out an automated failback process, with the Reprotect button inverting the replication direction (see Figure 9.31).



**Figure 9.29** Although some array managers ask for the Recovery Site's IP and authentication details, you still must configure the Recovery Site SRA.



**Figure 9.30** Enabling the configuration of the EMC Celerra



**Figure 9.31** The SRM interface shows the replication direction, and is useful when monitoring failover and failback procedures.

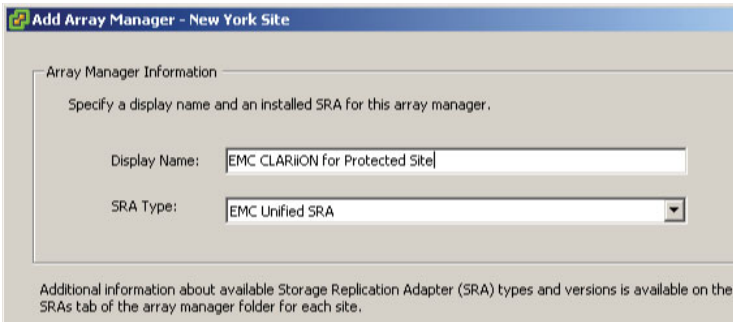
## Configuring Array Managers: EMC CLARiiON

EMC has one SRA that covers both the Unisphere range of arrays and the newer VMX series of systems together with “enabler” software for particular types of replication. So, regardless of the generation you possess, you should be able to install and configure it. Installing the EMC SRA VNX Replicator is a relatively simple affair. In this section, I will walk you through the configuration of the EMC CLARiiON with VMware SRM.

With EMC CLARiiON systems the SRM server will communicate to the CLARiiON at the Protected Site (New York) to collect volume information. It’s therefore necessary to configure a valid IP address for the SRM to allow this to occur *or* allow routing/intra-VLAN communication if your SRM and VSA reside on different networks. This is one of the challenges of installing your SRM and vCenter on the same instance of Windows. Another workaround is to give your SRM two network cards: one used for general communication and the other used specifically for communication to the CLARiiON. If you have no communication between the SRA and the CLARiiON you will receive an error message. Before you begin, it’s a good idea to confirm that you can ping both the Protected Site array and the Recovery Site array with the CLARiiON SP A and SP B ports’ IP address from the Protected Site (New York) SRM server.

To configure the array manager for the EMC CLARiiON, resume with these steps.

5. In the Add Array Manager dialog box, enter a friendly name for this manager, such as “EMC Clariion for Protected Site”.
6. Select EMC Unified SRA as the SRA Type, as shown in Figure 9.32.



**Add Array Manager - New York Site**

Array Manager Information

Specify a display name and an installed SRA for this array manager.

Display Name:

SRA Type:

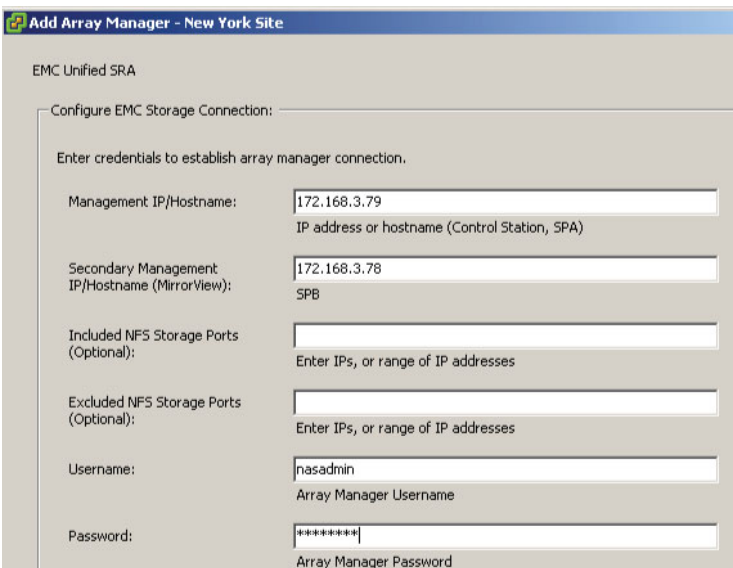
Additional information about available Storage Replication Adapter (SRA) types and versions is available on the SRAs tab of the array manager folder for each site.

**Figure 9.32** If you have many CLARiiON systems you might want to develop a naming convention that allows you to uniquely identify them.

7. Enter the IP address of the storage processors (SPA and SPB) at the Protected Site in the IP Address field—in my case, this is my New York CLARiiON system with the IP addresses 172.168.3.79 and 172.168.3.78.

If you are unsure of the IP address of the storage processors for your system, you can locate it in the Unisphere management pages under System Information.

8. Supply the username and password for the CLARiiON together with the IP address for the SPA and SPB (see Figure 9.33).



**Add Array Manager - New York Site**

EMC Unified SRA

Configure EMC Storage Connection:

Enter credentials to establish array manager connection.

Management IP/Hostname:   
IP address or hostname (Control Station, SPA)

Secondary Management IP/Hostname (MirrorView):   
SPB

Included NFS Storage Ports (Optional):   
Enter IPs, or range of IP addresses

Excluded NFS Storage Ports (Optional):   
Enter IPs, or range of IP addresses

Username:   
Array Manager Username

Password:   
Array Manager Password

**Figure 9.33** The IP address for SPA and SPB on the New York CLARiiON

These dialog boxes occasionally require you to scroll down in order to see all the fields.

- Click Next and then Finish. Once the array manager configuration for the Protected Site is added, you should also add the array manager configuration for the Recovery Site, as shown in Figure 9.34.

The next step is to enable the configuration, as shown in Figure 9.35. If you have used SRM before you will recognize this is a new step in the array manager configuration. It's designed to give the SRM administrator more control over the array pairs than was previously possible. If you do not enable the pairing you will be unable to successfully create Protection Groups.

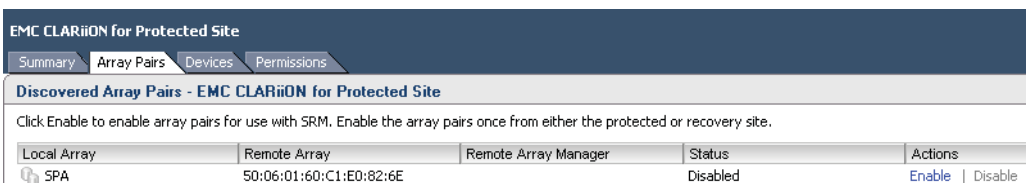
- To enable the configuration select the Array Pairs tab on the array configuration object and click the Enable link under the Actions column.

Occasionally, I've had to click Enable twice. This appears to be an issue with the way SRM refreshes this page. Once the array manager configuration is in use by Protection Groups it cannot be disabled.

This will complete the Remote Array Manager column with the name of the array configuration for the Recovery Site. If you look under the Devices tab you should see the volumes you are replicating to the Recovery Site. Notice how the device or volume is local to the New York Site. Also notice how the blue arrow indicates the volume is being replicated to the remote location of New Jersey. This arrow changes direction when you carry out an automated failback process, with the Reprotect button inverting the replication direction (see Figure 9.36).

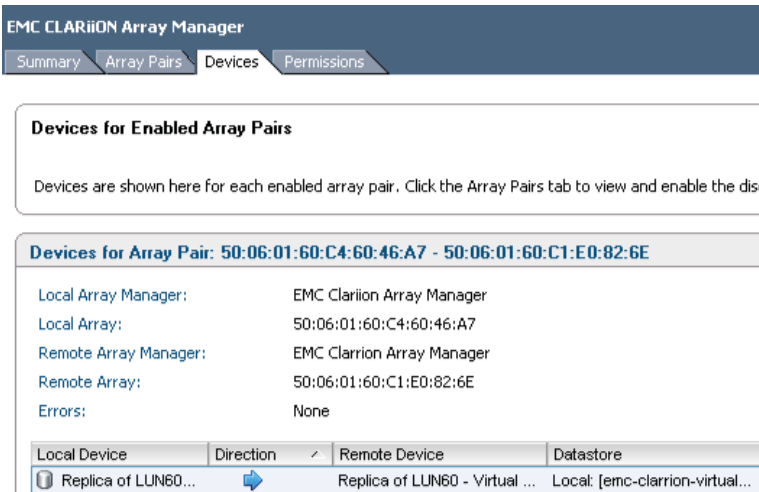


**Figure 9.34** Although some array managers ask for the Recovery Site's IP and authentication details, you must configure the Recovery Site SRA.



**Figure 9.35** Enabling the configuration on the EMC CLARiiON



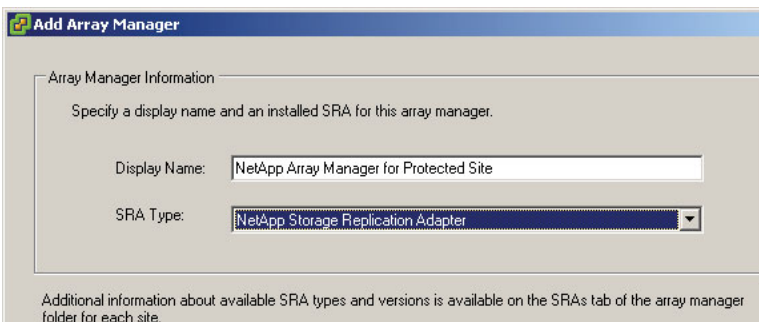


**Figure 9.36** SRM can show the replication direction, and is useful when monitoring failover and fallback procedures.

## Configuring Array Managers: NetApp FSA

To configure the array manager for the NetApp FSA, resume with these steps.

5. In the Add Array Manager dialog box, enter a friendly name for this manager, such as “NetApp Array Manager for Protected Site”.
6. Select NetApp Storage Replication Adapter as the SRA Type, as shown in Figure 9.37.
7. Enter the IP address of the group at the Protected Site in the IP Address field—in my case, this is my New York NetApp system with the IP address of 172.168.3.89



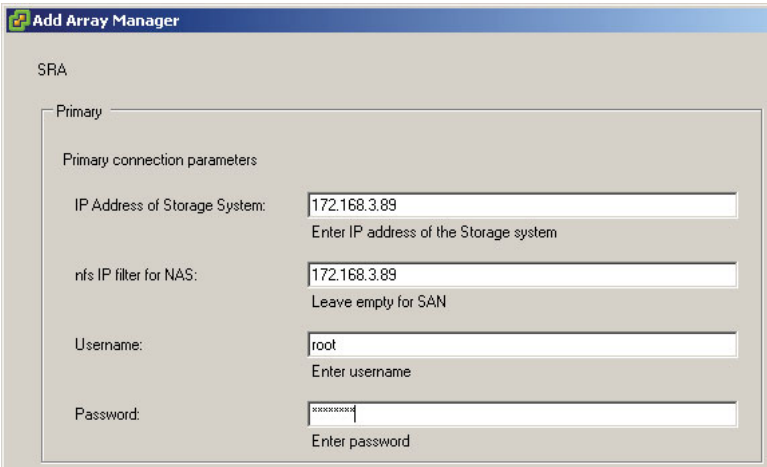
**Figure 9.37** The NetApp SRA uses signal configuration for all its supported storage protocols.

(see Figure 9.38). I used the same IP address for the system as the NFS IP filter for NAS. This may not be the case in larger production systems where the management traffic is placed on separate network interfaces.

8. Supply the username and password for the NetApp filer.

These dialog boxes occasionally require you to scroll down in order to see all the fields.

Most customers like to have separate networks for management and data traffic. This is mainly for security reasons, but performance can also be a concern. Many storage admins will use the management network to copy their own data around, such as software packages, service packs, and firmware updates. When the SRA interrogates the NetApp system, it may find a bunch of interfaces using various address ranges. And when SRM interrogates vCenter, it may find a bunch of ESX VMkernel interfaces using various address ranges. So it's entirely possible that when SRM needs to mount an NFS datastore (either the SnapMirror destination volume in a real failover, or a FlexClone of that volume in a test failover), it may choose to use an IP address range such as, for example, the management network. NetApp added the NFS filter to ensure that the SRA only reports the desired addresses back to SRM, which would mean that SRM can only choose the IP network you specify. You can actually specify multiple IP addresses if you need to; just separate them with a comma—for example, 192.168.3.88,192.168.3.87. In my case, I have a much simpler configuration where my management network and my NFS network are the same set of team NICs in the filer.



The screenshot shows a dialog box titled "Add Array Manager" with a "SRA" section. Under "Primary", there are four fields for "Primary connection parameters":

Field Label	Value	Placeholder/Instructions
IP Address of Storage System:	172.168.3.89	Enter IP address of the Storage system
nfs IP filter for NAS:	172.168.3.89	Leave empty for SAN
Username:	root	Enter username
Password:	XXXXXXXXXX	Enter password

**Figure 9.38** Entering the IP address of the group at the Protected Site

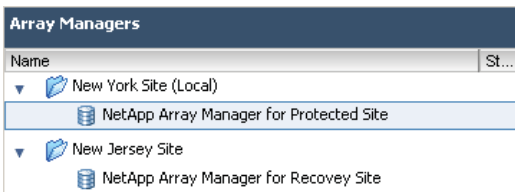
- Click Next and then Finish. Once the array manager configuration for the Protected Site is added, you should also add the array manager configuration for the Recovery Site (see Figure 9.39).

The next step is to enable the configuration. If you have used SRM before you will recognize this is a new step in the array manager configuration. It's designed to give the SRM administrator more control over the array pairs than was previously possible. If you do not enable the pairing you will be unable to successfully create Protection Groups.

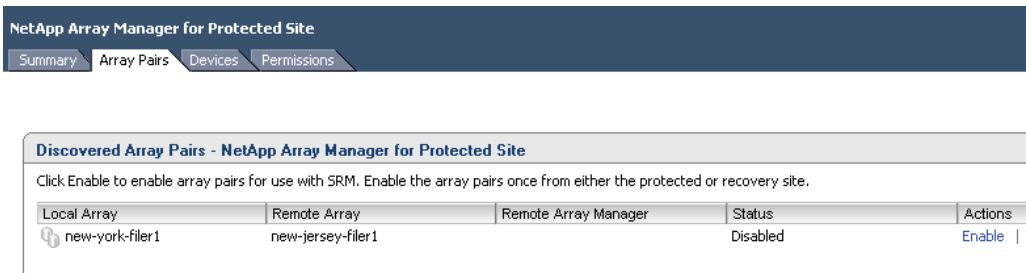
- To enable the configuration select the Array Pairs tab on the array configuration object and click the Enable link under the Actions column (see Figure 9.40).

Occasionally, I've had to click Enable twice. This appears to be an issue with the way SRM refreshes this page. Once the array manager configuration is in use by Protection Groups it cannot be disabled.

This will complete the Remote Array Manager column with the name of the array configuration for the Recovery Site. If you look under the Devices tab you should see the volumes you are replicating to the Recovery Site. Notice how the device or volume is local to the New York Site. Also notice how the blue arrow indicates the volume is being replicated to the remote location of New Jersey. This arrow changes direction when you carry out an automated failback process, with the Reprotect button inverting the replication direction (see Figure 9.41).



**Figure 9.39** If you have multiple arrays, consider a naming convention that allows you to uniquely identify each system.



**Figure 9.40** Enabling the configuration in NetApp FSA

The screenshot shows the NetApp Array Manager for Protected Site interface. The top navigation bar includes tabs for Summary, Array Pairs, Devices, and Permissions. The main content area is titled "Devices for Enabled Array Pairs" and contains a sub-section for "Devices for Array Pair: new-york-filer1 - new-jersey-filer1".

Key configuration details shown:

- Local Array Manager: NetApp Array Manager for Protected Site
- Local Array: new-york-filer1
- Remote Array Manager: NetApp Array Manager for Recovery Site
- Remote Array: new-jersey-filer1
- Errors: None

A table below these details shows the replication direction:

Local Device	Direction	Remote Device	Datastore
/vol/vol1_virtualm...	➔	/vol/vol1_replica_of_virtualmachines	Local: [netapp-virtualmachines]

**Figure 9.41** SRM can show the replication direction, and is useful when monitoring failover and failback procedures.

## Creating Protection Groups

Once you are satisfied with your array manager configuration you're ready to carry on with the next major step: configuring Protection Groups. Protection Groups are used whenever you run a test of your Recovery Plan, or when DR is invoked for real. Protection Groups are pointers to the replicated vSphere datastores that contain collections of virtual machines that will be failed over from the Protected Site to the Recovery Site. The Protection Groups' relationships to ESX datastores can be one-to-one. That is to say, one Protection Group can contain or point to one ESX datastore. Alternatively, it is possible for one Protection Group to contain many datastores—this can happen when a virtual machine's files are spread across many datastores for disk performance optimization reasons or when a virtual machine has a mix of virtual disks and RDM mappings. In a loose way, the SRM Protection Group could be compared to the storage groups or consistency groups you may create in your storage array. However, what actually dictates the membership of a Protection Group is the way the virtual machines utilize the datastores.

### TIP

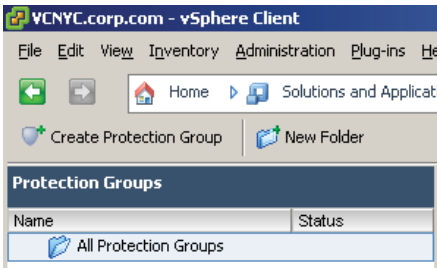
When you create your first Protection Group you might like to have the vSphere client open on both the Protected Site vCenter and the Recovery Site vCenter. This will allow you to watch in real time the events that happen on both systems. Of course, if you are running in linked mode you will see this happening if you expand parts of the inventory.

To configure Protection Groups follow these steps.

1. Log on with the vSphere client to the Protected Site's vCenter (New York).
2. Click the Site Recovery icon.
3. Select the Protection Groups pane and click the Create Protection Group button, as shown in Figure 9.42.

New to this release is the ability to create folders in the Protection Groups, to allow you to more easily lay out your Protection Groups if you have a significant number of them.

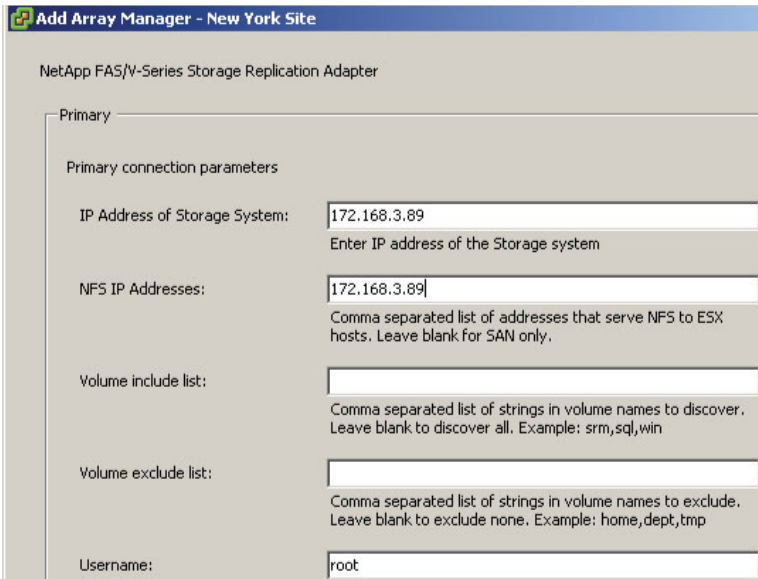
4. In the Create Protection Group dialog box (whether you are using VR or array-based replication), if you have more than one array manager select the one associated with this Protection Group, as shown in Figure 9.43. Then select the pairing of arrays contained within the array manager configuration.
5. Click Next. This should enumerate all the volumes discovered on the arrays in question. If you select the volume names, you should see the VMs contained within those ESX datastores (see Figure 9.44).



**Figure 9.42** You can now create both Protection Groups and Protection Group folders.



**Figure 9.43** The EMC Celerra array manager configuration. You may have many array pairs, each hosting many datastores protected by replication.

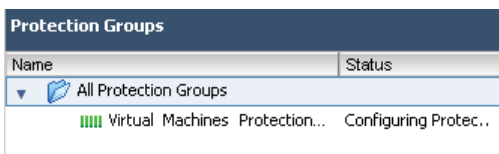


**Figure 9.44** Dell EqualLogic datastore containing a number of virtual machines

6. In the Create Protection Group Name and Description dialog box, enter a friendly name and description for your Protection Group. In my case, I'm creating a Protection Group called "Virtual Machines Protection Group." Click Finish.

At this point, a number of events will take place. First, as the Protection Group is being created the icon of the Protection Group changes, and its status is marked as "Configuring Protection," as shown in Figure 9.45. Second, at the Recovery Site vCenter you will see the task bar indicate that the system is busy "protecting" *all* virtual machines that reside in the datastore included in the Protection Group (see Figure 9.46).

Meanwhile, the Recovery Site's vCenter will begin registering the placeholder VMX files in the correct location in the inventory, as shown in Figure 9.47. As you can see, each



**Figure 9.45** When Protection Groups are first created their status is modified to "Configuring Protection."

Recent Tasks	
Name	Target
Protect VM	ss02
Protect VM	ss01
Protect VM	mail03
Protect VM	mail02
Protect VM	mail01
Protect VM	fs03
Protect VM	fs02

**Figure 9.46** During the creation of Protection Groups each affected VM has a task associated with it.

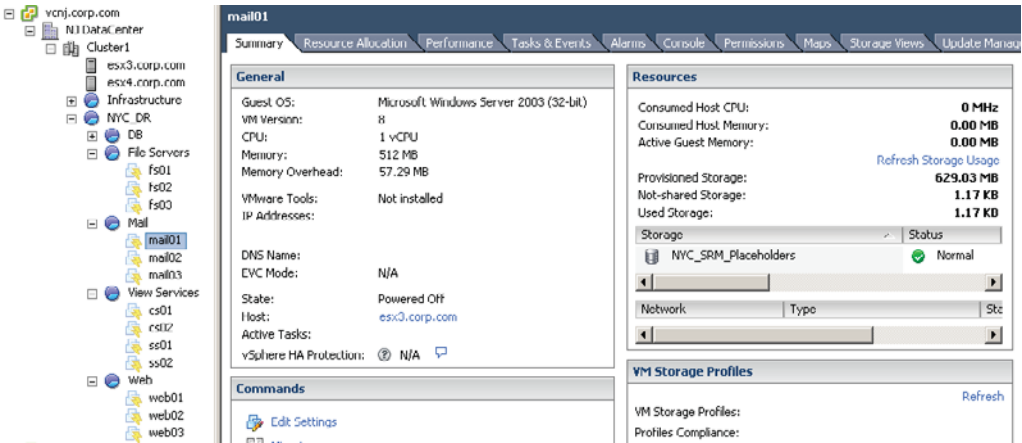
Recent Tasks	
Name	Target
Create virtual machine	File Servers
Create virtual machine	View Services
Create virtual machine	View Services
Create virtual machine	File Servers
Create virtual machine	File Servers
Create virtual machine	View Services
Create virtual machine	Mail
Create virtual machine	Web
Create virtual machine	Web
Create virtual machine	Mail
Create virtual machine	View Services
Create virtual machine	Mail

**Figure 9.47** The Recovery Site's vCenter begins registering the placeholder VMX files in the correct location in the inventory.

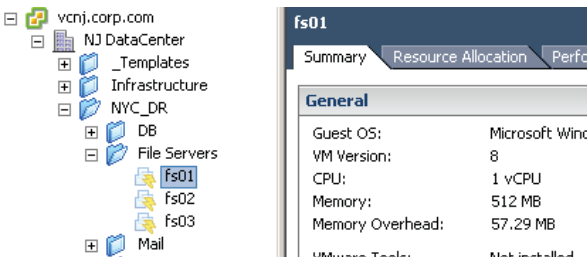
Protect VM event has a “Create virtual machine” event. SRM isn't so much creating a new VM as it is registering placeholder VMs in the Recovery Site.

You will also have noticed these “new” VMs are being placed in the correct resource pool and folder. If you select one of the placeholder files you can see it only takes up a fraction of the storage of the original VM. You should also see that these placeholders have been given their own unique icon in the vCenter inventory at the Recovery Site. This is new to SRM. Previously, the placeholder VMs just had the standard “boxes in boxes” icon, and that made them difficult to identify. Even with the new-style icon, as shown in Figure 9.48, I still recommend a separate resource pool and/or folder structure so that you can keep these ancillary placeholders separate and distinct from the rest of your infrastructure.

If you browse the storage location for these placeholders you can see they are just “dummy” VMX files (see Figure 9.49). As I mentioned before, occasionally VMware SRM



**Figure 9.48** Creation of placeholder VMs with the new lightning bolt icon, which should make them easier to distinguish in the vCenter inventory

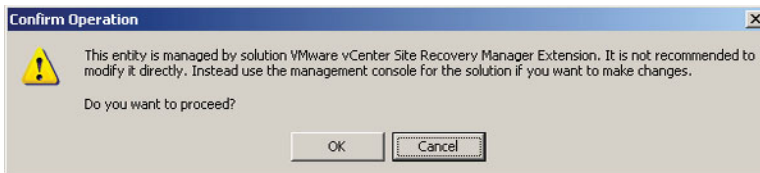


**Figure 9.49** Placeholder VMs are created in the datastore specified in the Placeholder tab on the properties of each site.

refers to these placeholder VMs as “shadow” VMs. In the Virtual Machines and Template view, at the Recovery Site’s vCenter the VMs have been allocated to the correct folder. SRM knows which network, folder, and resource pool to put the recovery VMs into, because of the default inventory mapping settings we specified earlier.

You should know that if you create a template and store it on a replicated datastore it will become protected as well. This means templates can be recovered and be part of Recovery Plans (covered in Chapter 10) just like ordinary VMs. Templates are not powered on when you run a Recovery Plan, because they can’t be powered on without being converted back to being a virtual machine. As you can see, these placeholder VMs are very different from the VMs you normally see registered to vCenter. If you try to edit them like any VM you will be given a warning (shown in Figure 9.50) that this is not a recommended action.





**Figure 9.50** The warning dialog box that appears if you try to edit the placeholder VMs listed in the Recovery Site

### WARNING

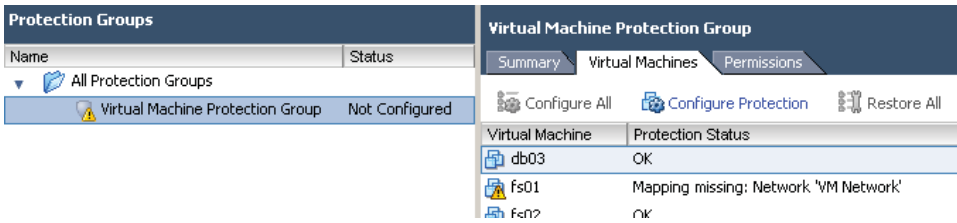
Deleting Protection Groups at the Protected Site vCenter reverses this registration process. When you delete a protected group, it unregisters and destroys the placeholder files created at the Recovery Site. This does not affect the replication cycle of the virtual machines that are governed by your array's replication software. Be very cautious when deleting Protection Groups. The action can have unexpected and unwanted consequences if the Protection Groups are "in use" by a Recovery Plan. This potential problem is covered later in this book. To understand it at this point in the book would require additional details regarding Recovery Plans that we have not yet discussed. For now, it's enough to know that if you delete Protection Groups the placeholders get deleted too, and all references to those VMs in the Recovery Plan get removed as well!

## Failure to Protect a Virtual Machine

Occasionally, you might find that when you create a Protection Group the process fails to register one or more virtual machines at the Recovery Site. It's important not to overreact to this situation as the causes are usually trivial ones caused by the configuration, and they are very easy to remedy. The most common cause is either bad inventory mappings, or a VM that falls outside the scope of your inventory mappings. In this section I will give you a checklist of settings to confirm, which will hopefully fix these problems for you. They amount to the kind of initial troubleshooting you may experience when you configure SRM for the first time.

### Bad Inventory Mappings

This is normally caused by a user error in the previous inventory mapping process. A typical failure to protect a VM is shown in Figure 9.51. The error is flagged on the Protected Site with a yellow exclamation mark on the Protection Group, and the virtual machines that failed to be registered.



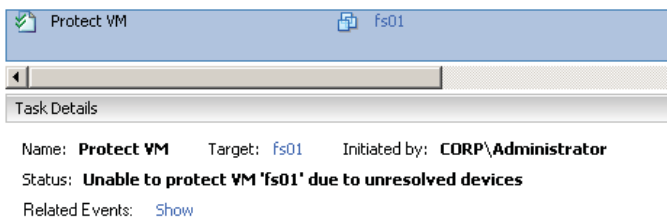
**Figure 9.51** A VM failing to be protected because the VM Network port group was not included in the inventory mappings

As a consequence, you will also see errors in the Tasks & Events tab for the affected VMs. The classic clue that a VM has a bad inventory mapping is the “Unable to protect VM <VM name> due to unresolved devices” message shown in Figure 9.52.

This error is usually caused by the virtual machine settings being outside the scope of the inventory mapping settings defined previously, and therefore the Protection Group doesn’t know how to map the virtual machine’s current folder, resource pool, or network membership to the corresponding location at the Recovery Site. A good example is networking, which I just described above.

In the inventory mapping process, I did not provide any inventory mappings for the VM Network port group. I regarded this as a local network that contained local virtual machines that did not require protection. Accidentally, the virtual machine named “fs01” was patched into this network, and therefore did not get configured properly in the Recovery Plan. In the real world this could have been an oversight; perhaps I meant to set an inventory mapping for vlan10 but forgot to. In this case, the problem wasn’t my virtual machine but my bad configuration of the inventory mapping.

Another scenario could be that the inventory mapping is intended to handle default settings where the rule is always *X*. A number of virtual machines could be held within the Protection Group and could have their own unique settings; after all, one size does



**Figure 9.52** The unresolved devices error that usually indicates a problem with inventory mappings

not fit all. SRM can allow for exceptions to those rules when a virtual machine has its own particular configuration that falls outside the group, just like with users and groups.

If you have this type of inventory mapping mismatch it will be up to you to decide on the correct course of action to fix it. Only you can decide if the virtual machine or the inventory mapping is at fault. You can resolve this match in a few different ways.

- Update your inventory mappings to include objects that were originally overlooked.
- Correct the virtual machine settings to fall within the default inventory mapping settings.
- Customize the VM with its own unique inventory mapping. This does not mean you can have rules (inventory mappings) and exceptions to the rules (custom VM settings). A VM either is covered by the default inventory mapping or is not.

If you think the inventory mapping is good, and you just have an exception, it is possible to right-click the icon in the Protection Group, select **Configure Protection** in the menu that opens, and offer per-VM inventory settings. If you had a bigger problem—a large number of VMs have failed to be protected because of bad inventory mapping configurations—you can resolve that in the inventory mapping, and then use **Configure All** to try the protection process again.

I would say the most common reason for this error is that you have deployed a new VM from a template, and the template is configured for a network not covered by the inventory mapping. Another cause can concern the use of SvSwitches. It's possible to rename the port groups of an SvSwitch to be a different label. This can cause problems for both the inventory mapping and the affected VMs. As a consequence, when the Protection Groups are created for the first time the protection process fails because the inventory mapping was using the old name.

## Placeholder VM Not Found

Another error that can occur is if someone foolishly deletes the placeholder that represents a VM in the Recovery Site, as shown in Figure 9.53. It is possible to manually delete a placeholder VM, although you do get the same warning message as you would if you tried to edit the placeholder settings. Nonetheless, these placeholder objects are not protected from deletion. If a rogue vCenter administrator deletes a placeholder you will see a yellow exclamation mark on the Protection Group, together with a “Placeholder VM Not Found” error message.

The quickest way to fix this problem is to choose either the **Restore All** link or the **Restore Placeholder** link in the Protection Group interface. The **Restore All** option rebuilds all

Protection Groups		Virtual Machines Protection Group			
Name	Status				
▼ All Protection Groups					
Virtual Machines Prote...	Not Configured				

Virtual Machines Protection Group				
Summary				
Virtual Machines				
Permissions				
Configure All    Configure Protection    Restore All    Restore Placeholder				
Virtual Machine	Protection Status	Recovery Folder	Recovery Resour	
db01	OK	DB	DB	
db02	OK	DB	DB	
db03	OK	DB	DB	
fs01	Placeholder VM Not Found			
fs02	OK	File Servers	File Servers	

**Figure 9.53** The “Placeholder VM Not Found” error message caused by accidental deletion of the placeholder in the inventory

the placeholders within the Protection Group, whereas Restore Placeholder fixes just one selected placeholder in the list.

## VMware Tools Update Error—Device Not Found: CD/DVD Drive 1

Occasionally, the Protection Group can have a VM that displays an error on its own. For example, in Figure 9.54 the VM named “db01” has the error message “Device Not Found: CD-DVD drive1.” This error is relatively benign and does not stop execution of the plan.

This issue was created by a faulty VMware Tools update using Update Manager. The CD-ROM mounted was to a Linux distribution where an automatic mounting and update of VMware Tools failed. The Update Manager was unsuccessful in unmounting the .iso file at /usr/lib/vmware/isoimages/linux.iso, but the auto-execution of VMware Tools does not work in the same way with Linux as it does with Windows. With Linux all that happens is that the .iso file is mounted as a CD-ROM device, but it is up to the administrator to extract the .tgz package and install VMware Tools to the guest system. This error was resolved by right-clicking the affected VM, and under the Guest menu

Virtual Machines Protection Group			
Summary			
Virtual Machines			
Permissions			
Configure All    Configure Protection    Restore All    R			
Virtual Machine	Protection Status	Recover	
db01	Device Not Found: CD/DVD drive 1	DB	
db02	OK	DB	
db03	OK	DB	

**Figure 9.54** The old chestnut of connected CD/DVD drives can cause a benign error to appear on the Protection Group.

selecting “End VMware Tools install.” This triggered an unmounting of the VMware Tools .iso image.

## Delete VM Error

Occasionally, you will want to delete a VM that might also be a member of a Protection Group. The correct procedure for doing this is to unprotect the VM, which will then unregister its placeholder VMX file, and as a consequence remove it from any Recovery Plan. Of course, there’s nothing to stop someone from ignoring this procedure and just deleting the VM from the inventory. This would result in an “orphaned” object in the Protection Group and Recovery Plan, as shown in Figure 9.55.

Virtual Machine	Protection Status	Recovery Folder	Recovery Resource Pool	Recovery Plan
db03	Invalid: Protected VM deleted.	DB	DB	Cluster1
fs02	Invalid: Protected VM deleted.	File Servers	File Servers	Cluster1

**Figure 9.55** The error when a VMware administrator deletes a protected VM without first unprotecting it in SRM

To fix these VMs, select the affected VM and click the Remove Protection button.

## It’s Not an Error, It’s a Naughty, Naughty Boy!

If you can forgive the reference to Monty Python’s *The Meaning of Life*, the confusing yellow exclamation mark on a Protection Group can be benign. It can actually indicate that a new virtual machine has been created that is covered by the Protection Group. As I may have stated before, simply creating a new virtual machine on a replicated LUN/volume does not automatically mean it is protected and enrolled in your Recovery Plan. I will cover this in more detail in Chapter 11, Custom Recovery Plans, as I examine how SRM interacts with a production environment that is constantly changing and evolving.

Hopefully with these “errors” you can begin to see the huge benefit that inventory mapping offers. Remember, inventory mappings are optional, and if you chose not to configure them in SRM when you created a Protection Group every virtual machine would fail to be registered at the Recovery Site. This would create tens or hundreds of virtual machines with a yellow exclamation mark, and each one would have to be mapped by hand to the appropriate network, folder, and resource pool.

## Summary

As you have seen, one of the biggest challenges in SRM in the post-configuration stages is network communication. Not only must your vCenter/SRM servers be able to communicate with one another from the Protected Site to the Recovery Site, but the SRM server must be able to communicate with your array manager also. In the real world, this will be a challenge which may only be addressed by sophisticated routing, NATing, intra-VLAN communication, or by giving your SRM server two network cards to speak to both networks.

It's perhaps worth saying that the communication we allow between the SRM and the storage layer via the vendor's SRA could be very contentious with the storage team. Via the vSphere client you are effectively managing the storage array. Historically, this has been a manual task purely in the hands of the storage team (if you have one), and they may react negatively to the level of rights that the SRM/SRA needs to have to function under a default installation. To some degree we are cutting them out of the loop. This could also have a negative impact on the internal change management procedures used to handle storage replication demands in the business or organization within which you work. This shouldn't be something new to you.

In my research, I found a huge variance in companies' attitudes toward this issue, with some seeing it as a major stumbling block and others as a stumbling block that could be overcome as long as senior management fully backs the implementation of SRM—in other words, the storage team would be forced to accept this change. At the opposite extreme, those people who deal with the day-to-day administration of storage were quite grateful to have their workload reduced, and noted that the fewer people involved in the decision-making process the quicker their precious virtual machines will be online.

Virtualization is a very political technology. As “virtualizationists” we frequently make quite big demands on our network and storage teams that can be deemed as very political. I don't see automating your DR procedures as being any less political. We're talking about one of the most serious decisions a business can take with its IT: invoking its DR plan. The consequences of that plan failing are perhaps even more political than a virtualization project that goes wrong.

Of course, it is totally impossible for me to configure every single storage vendor's arrays and then show you how VMware SRM integrates with them, but hopefully I've given you at least a feel for what goes on at the storage level with these technologies together with insight into how SRM configuration varies depending on your storage vendor's technology. I hope you have enough knowledge now to both communicate your needs to the storage guys as well as understand what they are doing at the storage level to make all this work. In the real world, we tend to live in boxes—I'm a server guy, you're a storage

guy, and he's a network guy. Quite frequently we live in ignorance of what each guy is doing. Ignorance and DR make for a very heady brew.

Lastly, I hope you can see how important inventory mappings and Protection Groups are going to be in the recovery process. Without them a Recovery Plan would not know where to put your virtual machines in vCenter (folder, resource pool, and network) and would not know on which LUN/volume to find those virtual machine files. In the next chapter we will look at creating and testing Recovery Plans. I'm going to take a two-pronged approach to this topic. Chapter 10 gets you up and running, and Chapter 11 takes Recovery Plans up to their fully functional level. Don't worry; you're getting closer and closer to hitting that button labeled "Test my Recovery Plan."

# Index

## A

---

- ABR. *See* Array-based replication
- Access control
  - add ESX hosts manually, 60–61
  - ESX host to HP VSA iSCSI target, 122–127
  - ESXi host to EqualLogic iSCSI volume, 26–31
  - ESXi host to NetApp iSCSI target, 142–147
  - iSCSI volume, 25–26
  - overview of, 368–370
  - SRM administrator, 370–372
  - vCenter linked mode impacting, 358
- Access tab, iSCSI volume, 25–26
- Active Directory
  - access control authentication, 369
  - configure VM power-on for Recovery Plan, 299
  - create SRM administrators delegation in, 370–372
  - PowerCLI supporting authentication, 322
- Active processes, testing Recovery Plan, 277
- Activities pane, Schedules option, 37–39
- Adapter ID column, .csv file, 334
- Add & Remove System link, Unisphere, 45–46
- Add Array Manager dialog box
  - EMC Celerra, 247
  - EMC CLARiiON, 251–252
  - NetApp FSA, 254
- Add Script dialog box, Recovery Plan, 326–327
- Add Send Target Server dialog box, iSCSI Initiator, 146
- Add Step button
  - command steps to Recovery Plan, 314
  - command steps with PowerCLI, 318, 320
  - prompt steps to Recovery Plan, 310–311
- Add Storage Controller Wizard, NetApp VSC, 156–157
- Add Storage Wizard, resignaturing VMFS volumes, 175–176, 427–428
- Add to Inventory Wizard, scripting recovery test, 429–430



- Administrator, create SRM, 370–371
- Advanced Settings
  - deploying VRS, 215–216
  - replicate iSCSI volumes, 35–36
  - retain original volume name during resignaturing, 177–178
  - site name changes, 191
  - SRM inventory options, 360–361
- Aggregates, NFS, 134
- Alarms
  - access control via, 369
  - create message, 364
  - create new VMs with, 362–363
  - create SRM service, 364–365
  - events covered by, 360–362
  - introduction, 357
- Alerts. *See also* Alarms
  - array manager configuration and, 242
  - create volumes and, 113
  - Protection Group, for new datastores being used by VMs, 346–347
  - resignature VMFS volumes and, 175
- All Systems pull-down list, 46, 74
- Architecture. *See* VMware SRM architecture
- Array-based replication
  - Dell EqualLogic. *See* Dell EqualLogic replication
  - EMC Celerra. *See* EMC Celerra replication
  - EMC CLARiiON MirrorView. *See* EMC CLARiiON MirrorView
  - HP StorageWorks P4000 VSA. *See* HP StorageWorks P4000 VSA
  - NetApp SnapMirror. *See* NetApp SnapMirror
  - scalability limits, 171
  - vSphere Replication. *See* VR (vSphere Replication)
- Array-based snapshots, Recovery Site test, 274–275
- Array manager configuration
  - Dell EquaLogic, 245–248
  - EMC Celerra, 248–251
  - EMC CLARiiON, 251–254
  - introduction, 241–244
  - NetApp FSA, 254–257
  - order of SRM, 342
  - process of, 244–245
  - at Protected Site, 375
  - at Protected Site, execute Recovery Plan, 401
  - Protection Groups, 258
  - refresh in bidirectional configurations, 378–379
  - remove when decommissioning site, 394
  - Repair Array Managers button
    - deprecated in, 354
    - upgrading SRM 4.1 to 5.0, 452–453
- Array Pairs tab
  - Dell Array Manager, 247
  - EMC Celerra Array Manager, 250–251
  - NetApp FSA Array Manager, 256
- Assign and Unassign Volumes and Snapshots, to ESX hosts, 120–122
- Asynchronous replication
  - configure HP VSA, 114–118
  - create EMC LUN, 78–79
  - create reserved LUN pool for, 75–78
  - vSphere Replication as, 202
- Authentication. *See also* SQL Authentication
  - Active Directory, 322
  - PowerCLI, 321–327
  - upgrading SRM 4.1 to 5.0, 452
- Auto Generate Target Qualified Names. *See* IQNs (Auto Generate Target Qualified Names)

Auto option, Create Recovery Plan Wizard, 271–272

Automated failback

- dangers of, 172–173
- new in SRM 5.0, 3
- Reprotect Mode speeding up, 3
- storage replication adapter and, 194
- VR not supporting for VMs, 204

## B

Backup

- configure VSA, 100
- limitations for disaster recovery, 5–6
- before upgrading to SRM, 451
- before upgrading VMware Tools, 455

Bandwidth

- configure VRMS, 212–214
- HP VSA control of, 115, 118–119
- NetApp SnapMirror at Recovery Site, 153–155
- Recovery Plan testing and, 227
- replication schedule based on, 39, 67–68, 70, 165
- save for large VMs during VR, 202
- save with physical couriering, 220
- SnapMirror control of, 150, 153–155
- virtualize production systems before DR
  - location and, 6
- VMware Fault Tolerance and, 9

Baselines, upgrade, 446–448

BC (business continuity), DR and, 10

Bidirectional configuration

- license SRM for, 179
- mutual reciprocal permissions, 369
- overview of, 164–165

Bidirectional relationships

- configure inventory mappings, 376–378
- control start-up order with vApp, 381–384

- create Protection Group, 380–381
- create Recovery Plan, 381
- overview of, 375–376
- refresh array manager, 378–379

Boot process, Recovery Plan. *See* Power on VMs

Boxes-in-boxes logo, shadow VMs, 408

Break Connections link, reverse pairing process, 230

Break VRMS connections, reverse pairing process, 214

Bubble networks, 236

Business continuity (BC), DR and, 10

## C

CamelCase, HP VSA management groups, 109

Cancel option, Recovery Plan test, 285

Case-sensitivity, replication partners, 32

Celerra Network Servers tab, Replication Wizard, 70–71

Celerra system. *See* EMC Celerra replication

Centralized Management Console. *See* CMC (Centralized Management Console), HP P4000

Certificates

- pairing process, 229–230
- SRM software installation, 188–190
- VRMS connections, 214–215
- vSphere client SRM plug-in installation, 196–197

CHAP

- create EqualLogic iSCSI volume, 25–26
- create iSCSI LUN, 61
- ESXi host access to EqualLogic iSCSI volume, 29

CHAP, *continued*

- ESXi host access to NetApp iSCSI target, 145
- not supported for SRM by HP VSA, 120

## CLARiiON systems

- EMC MirrorView. *See* EMC CLARiiON MirrorView
- replication technology for, 13

## Clean installs, vs. upgrades, 433–434

## Cleanup phase

- after Recovery Plan test, 283–285
- error when using iSCSI, 287–288
- Force Cleanup, 281, 289–290

## Client, upgrading vSphere, 441–442

## CLiQ, HP, 100

## Clones

- create multiple VSAs, 99
- manage storage when scripting recovery test, 425–426
- reset lab environments for VSAs, 99–100
- VR not protecting linked, 204

## Cloud, scalability for, 9–10

## Clusters

- configure HP VSA, 115–118
- create HP VSA, 111–112
- locate placeholder datastores in, 239
- rename in Protected Site, 339
- rename in Recovery Site, 342

## CMC (Centralized Management Console), HP P4000

- add to management groups, 108–111
- add VSAs to, 108
- configure HP VSA for replication, 114–118
- configure HP VSA with ESX hosts, 120–122
- create cluster, 111–112
- create test volume at Recovery Site, 127–129
- create volume, 113–115

- install, 107–108
- overview of, 97–98
- shutdown VSA, 129

## Cmdlets, testing SRM, 276

## Command-line switches, shared sites, 384–385

## Command steps

- add to Recovery Plan, 313–314
- add to Recovery Plan with PowerCLI, 315–321
- call scripts within guest OS via, 328–329
- reduce RAM in recovery with PowerCLI, 319–321

## Communication paths, SRM network, 161–164

## Compatibility matrix documents, VMware, 170

## Compellent Storage Center SRA, 195

## Complete Connections dialog box, pairing process, 229

## Configuration, HP VSA

- add to management console, 108
- add VSAs to management groups, 108–111
- allocate volumes to ESX hosts, 120–122
- cluster, 111–112
- ESX hosts, 120
- FAQ, 100
- for replication, 114–118
- settings and first-power-on, 103–104
- volume, 113–115
- VSA host, 105–107

## Configuration page, VRMS, 212–214

## Configure All button, new VM in Protection Group, 338

## Configure Connection Wizard, pairing process, 227–231, 392–393

## Configure on Recovery Site NetApp filer, SnapMirror, 150–155

- Configure Protection
    - manual IP guest customization, 331–332
    - Protection Groups, 264
  - Configure Recovery, manual IP guest
    - customization, 331–332
  - Configure Replication dialog box, VR, 218
  - Configure VRMS connection link, 214–215
  - Confirmation text, e Recovery Plan, 402
  - connect-viserver cmdlets, command steps, 315–316
  - Connection Count, database configuration, 192
  - Connections
    - configure VRMS, 214–215
    - between Protected and Recovery Site SRMs, 226–231
    - reverse pairing process by breaking, 214, 230
    - SRM server failures, 198–199
  - Consistency, file level, 11–12
  - Consistency groups
    - create, 88–89
    - overview of, 75
    - store VMs on multiple datastores and, 348
  - Contact information, replication partners, 33
  - CPU requirements, HP P4000 VSA, 99
  - Create LUN dialog box, EMC LUN, 76–77, 79–80
  - Create LUN link, iSCSI LUN, 59
  - Create Mirror Wizard, NetApp
    - SnapMirror, 152–155
  - Create Multiple LUNS, iSCSI LUN, 60–61
  - Create Remote Mirror, EMC MirrorView, 80–82
  - Create Secondary Image LUN, EMC
    - MirrorView, 83
  - Create Snapshot, EMC MirrorView, 86–88
  - Create Volume dialog box, NetApp
    - SnapMirror, 135
  - Credentials
    - array manager communications and, 242
    - configure VRMS, 213
    - NetApp SnapMirror, 152
    - pairing process, 229–231
    - SRM software installation, 186–187
    - vCenter linked mode, 359
  - .csv files
    - add VMs to inventory for scripting
      - recovery test, 429–430
    - for bulk changes to IP, 332–336
    - IP address changes in Recovery VMs, 329–330
    - PowerCLI variables in Recovery Plan, 325–327
    - script variables in, 324–325
  - Custom Recovery Plans. *See* Recovery Plans, custom
  - Customize IP step, manual IP guest, 331–332
- ## D
- 
- Data Mover, Celerra
    - conduct ping test, 64
    - create interconnects for replication, 66–68, 70–71
    - create iSCSI LUN, 59–60
    - create iSCSI target, 46–51
    - defined, 44
    - hold new file system with, 56–57
  - data source name (DSN) connection, 184–185, 192
  - Database
    - configure for VRMS, 206–208
    - control how VMs power-on for recovery of, 299
    - upgrading vCenter, 438–439

- Database, *continued*
  - upgrading VUM back-end, 443–444
  - upgrading with SRM installer, 452–453
- Database, VMware SRM installation
  - communication role, 162–163
  - configure DSN, 184–185
  - create, 181–184
  - install SRM server, 192–193
- Datacenters
  - decommissioning, 394
  - pairing. *See* Bidirectional configuration
  - placeholder datastores in, 239
  - rename in Protected Site, 339
  - rename in Recovery Site, 342
  - VRS in folders or, 216
- Datastores
  - add VMs to inventory, 429–430
  - assign placeholder, 237–241
  - clean up after failover, reprotect and failback, 414–415
  - deploy VRMS, 209
  - HP VSA on, 102
  - multiple, 346–348, 350–351
  - within Protection Groups, 257–261
  - update for bidirectional configurations, 378–379
  - vSphere renaming issues, 342
  - vSphere Replication and, 218, 221–222
- Dates, configure replication schedule, 38
- Decommissioning sites, 394
- Dekens, Luc, 423, 431–432
- Delegate Reservation, EqualLogic
  - replication, 33, 35
- Deletion
  - accidental placeholder VM, 264–265
  - of protected VM error, 266
  - of Protection Groups, 262
- Dell EqualLogic
  - configure array manager, 245–248
  - configure VRMS connection, 214–215
  - planned recovery, 404–405
  - Recovery Plans tests, 291–292
  - reprotect process, 413
- Dell EqualLogic replication
  - getting started, 21–23
  - grant ESXi host access to iSCSI volume, 26–31
  - Host Integration for VMware edition, 39–42
  - for iSCSI volume, 23–26, 34–37
  - partners, 32–34
  - schedule, 37–39
- Destination Settings, Celerra Replication Wizard, 67, 69
- Destination Volume page, NetApp SnapMirror, 153–154
- Direction error, redirect process, 411–412
- disaster recovery (DR)
  - life before VMware SRM, 5–7
  - technology not for, 7–10
- disconnect statement, reducing RAM in recovery, 316–321
- Distributed Resource Scheduler (DRS), 8, 299–302
- Distributed vSwitches. *See* DvSwitches (Distributed vSwitches)
- DM Interconnects tab, Replication Wizard, 70–71
- DNS (Domain Name Server)
  - authentication in access control, 369
  - configure bulk changes to IP addresses, 334–335
  - configure for NetApp SnapMirror, 148
  - configure VM power-on for Recovery Plan, 299
  - execute Recovery Plan, 400
- DNS name resolution
  - failure to connect to SRM server and, 198
  - pairing process failure and, 227
  - in VMware SRM architecture, 167

Documentation, storage vendor, 14

Domain controllers, configure VM power on, 299

dr-customizer.exe utility, 332

DR (disaster recovery)

- life before VMware SRM, 5–7
- technology not for, 7–10

dr-ip-customizer command, 335

dr-ip-exporter utility

- configure bulk changes to IP, 332–336
- for guest customizations, 4
- srn-migration tool supporting, 454

DRS (Distributed Resource Scheduler), 8, 299–302

DSN (data source name) connection, 184–185, 192

DvSwitches (Distributed vSwitches)

- Dell EqualLogic replication, 27
- EMC Celerra replication, 51–52
- HP VSA replication, 123, 339–340
- mapping between SvSwitches and, 237
- NetApp SnapMirror replication, 142–143
- scripting recovery test, 430–431
- select network port group for VSA, 103
- upgrading SRM 4.1 to 5.0, 462

Dynamic Discovery tab, iSCSI Initiator Properties, 29–30, 144–146

## E

Edit Alarm dialog box, 364–365

Edit License Key dialog box, HP VSA, 113–114

Email

- configure power on for Recovery Plan, 299
- create SRM service alarm, 364–365

EMC

- overview of, 73–74
- Solutions Enabler, 93
- synchronous replication, 119
- VMX SRA, 194
- VNX Replicator Enabler, 194

EMC Celerra replication

- array manager configuration, 248–251
- configure, 64–71
- create iSCSI LUN, 59–63
- create iSCSI target, 46–51
- create new file system, 56–59
- grant ESX host access to iSCSI target, 51–56
- overview of, 43–46
- and testing plans, 292–293

EMC CLARiiON

- array manager configuration, 251–254
- RAID groups, 44

EMC CLARiiON MirrorView

- configure EMC MirrorView, 80–85
- create consistency groups, 88–89
- create EMC LUN, 78–80
- create reserved LUN pool, 75–78
- create snapshot for SRM tests, 85–88
- defined, 13
- grant ESX host access to CLARiiON LUNs, 90–93
- overview of, 73–75
- VSI plug-in, 93–95

Ephemeral ports, upgrading vCenter, 441

EqualLogic. *See* Dell EqualLogic

Errors

- after unplanned failover and loss of Protected Site, 417–418
- Protection Group configuration, 262–266
- Recovery Plan history, 368
- Recovery Plan test, 277
- redirect process direction, 411–412
- SRM server connectivity, 198–199
- upgrading vCenter, for FQDN, 440
- VM mapping, 336

- escfg-volume command, resignaturing
  - VMFS volumes, 427
- ESX 5 DVD installer, 446
- ESX hosts
  - access to EqualLogic iSCSI volume, 26–31
  - assign placeholder datastores, 238–241
  - Celerra system registered alongside, 44, 46
  - configure HP VSA, 102, 120–122
  - create EqualLogic iSCSI volume, 23–26
  - create iSCSI LUN, 60, 62
  - create NetApp volumes, 139–141
  - grant access to CLARiiON LUNs, 90–93
  - grant access to EMC Celerra iSCSI target, 51–56
  - grant access to HP VSA iSCSI target, 122–127
  - grant access to NetApp iSCSI target, 142–147
  - port groups and, 339
  - provision NetApp NFS storage for ESXi, 133–138
  - Recovery Plan and storage array vendors, 291–294
  - restart VMs with HA after failure, 8–9
  - scripting recovery for test, 425–427
  - storage management systems and, 15
  - test Recovery Plan, 278–279
  - test scripting recovery, 429–430
  - test storage configuration at Recovery Site, 273–275
  - upgrading, 445–451
  - upgrading vCenter, 438–439
  - VMware Fault Tolerance for, 9
- esxcfg-volumes command, resignaturing
  - VMFS volumes, 175–176
- Export, Recovery Plan history, 367–368
- Exports, scripting recovery test by
  - mounting NFS, 428

## F

---

- Failback
  - automated, 3, 407–415
  - bidirectional configurations and, 376–378
  - configure replication of iSCSI volume, 35–36
  - designing, 172–173
  - modify recovered VMs with PowerCLI and, 327
  - overview of, 397–400
  - planned, after disaster, 419–420
  - Reprotect Mode speeding up, 3
  - test of, 88
- FailBackMemory variable, 325–327
- Failover
  - clean up after, 414–415
  - designing, 172–173
  - unidirectional, 164
  - unplanned, Protected Site is lost, 415–419
- Failover, planned
  - Del EqualLogic and, 404–405
  - NetApp and, 405–406
  - overview of, 397–400
  - Protected Site is available, 400–404
- FailOverMemory variable, 325–327
- Falcon Storage SRA, 195
- False positives, and testing SRM, 276
- FAQs, HP P4000 VSA, 98–100
- Fault tolerance, 9, 204
- Fibre Channel protocol
  - create NetApp volumes for, 139–141
  - grant ESXi host access to NetApp iSCSI target, 146
  - test Recovery Plan, 278
- File level consistency, 11–12
- File system, Celerra, 56–60

FilerView  
 NetApp and testing plans, 294  
 NetApp System Manager replacing,  
 132–133

Find Systems Start wizard, add VSAs,  
 108

Firewalls  
 ESX host access to HP VSA iSCSI  
 target, 124  
 ESXi host access to NetApp iSCSI  
 target, 143  
 network communication issues, 164  
 pairing process failure and, 227

FlexClone, 294

FlexVols, 134–137

Folder mappings  
 bidirectional configurations, 376–378  
 Protected Site, 235

Folders  
 Protection Group, 380  
 Recovery Plan, 270, 381  
 rename in Protected Site, 339  
 rename in Recovery Site, 342

Force Cleanup, after Recovery Plan test,  
 281, 283–285

Format, exporting Recovery Plans, 366

FQDNs (fully qualified domain names)  
 add ESX host in HP VSA, 120  
 for HP management tools, 107  
 NetApp SnapMirror configuration, 138,  
 144–145, 148–150  
 pairing process configuration, 228–230  
 run Linked Mode Wizard, 358–359  
 vCenter upgrade process, 440  
 VMware SRM installation, 167, 186,  
 189–190

Frequency, replication schedule, 37–39

FT (fault tolerance), 9, 204

Full provisioned volumes, 113

---

## G

get-vm cmdlet, 317

Goal, of VMware SRM, 10

Group Manager, EqualLogic replication,  
 23–26, 31–34

Groups  
 configure array manager for Dell, 245  
 configure EqualLogic replication,  
 22–23  
 configure replication partners, 32–34  
 consequences of, 16  
 how storage management systems work,  
 14–16  
 Protection, 18–19  
 VM Dependencies showing VM, 4

Guest-connected storage, limitations,  
 133–134

Guest customization  
 bulk changes to IP addresses, 4,  
 332–336  
 manual IP, 330–332

Guest operating system, calling scripts  
 within, 328–329

Guest Shutdown option, Recovery Plan  
 test, 306

Guided Consolidation, 436

---

## H

HA clusters, 8–9

Hardware  
 resolve issues with RDM, 349  
 upgrading SRM 4.1 to 5.0, 458–460  
 VMware SRM requirements, 169–171

History, viewing Recovery Plan, 367–368

HIT-VE (Host Integration for VMware  
 Edition), 39–42



**Hostname**

- configure pairing process, 228
- configure VSA host, 105–107

**HP CLIQ, 100****HP SRA, installing, 195–196****HP StorageWorks P4000 VSA (virtual storage appliance)**

- add ESX hosts, 120
- add to management console, 108
- add to management groups, 108–111
- add volumes to ESX hosts, 120–122
- configure for replication, 114–118
- create cluster, 111–112
- create test volume at Recovery Site, 127–129
- create volume, 112–113
- FAQs about, 98–100
- grant ESX host access to HP VSA iSCSI target, 122–127
- importing, 100–103
- install management client, 107
- license for, 113–114
- modify settings and first-power-on configuration, 103–105
- monitor iSCSI connections, 127
- monitor replication/snapshot, 118–119
- overview of, 97–98
- primary configuration of VSA host, 105–107
- shutdown, 129
- test storage configuration at Recovery Site, 274

**HTTP listener port, SRM software installation, 191****I**

---

**IBM System Storage SAN Volume**

Controller SRA, 195

Image, ESX host upgrade, 446

**Import**

- ESXi Image, 446
- StorageWorks P4000 VSA, 100–103

**Installation, VMware SRM. *See* Database, VMware SRM installation; VMware SRM architecture****Interconnect Bandwidth Schedule, Replication Wizard, 67–68****Interface**

- EMC Unisphere tab, 48
- select for replication traffic, 67

**Internal network, scripting site recovery, 428–429****Inventory mappings**

- avoid casual removal of, 343
- bidirectional configurations, 376–378
- configure at Protected Site, 231–234, 375
- customize, 336–337
- failure, 262–264
- folder mappings, 235
- importance of, 266, 268
- network mappings, 236–237
- order of configuration of SRM, 343
- Protection Groups using, 225, 337–338
- resource mappings, 234–235

**Inventory objects, managing changes at Protected Site, 338–342****Inventory, scripting recovery test, 429–430****Inventory service, upgrading vCenter, 440****Invoke-VMscript cmdlet, PowerCLI, 328–329****IP addresses**

- array manager configuration. *See* Array manager configuration
- Dell EqualLogic replication, 27, 29–30, 32
- deploying VRMS, 210–211
- EMC Celerra replication, 47–50, 54–55, 65–71
- HP VSA configuration, 4–5, 105–107, 125–126

NetApp SnapMirror configuration,  
135–138, 144–150

pairing process configuration, 227–229

Recovery Plan execution and, 400

IP addresses, changing for recovery VMs

- configure bulk changes, 332–336
- create manual IP guest customization,  
330–332
- overview of, 329–330

IQNs (Auto Generate Target Qualified  
Names)

- Dell EqualLogic replication, 26
- EMC Celerra replication, 48–49, 54
- HP VSA configuration, 120
- naming convention for, 29
- NetApp SnapMirror configuration,  
139–140

iSCSI hardware adapter

- Dell EqualLogic replication, 26–31
- EMC Celerra replication, 51–56
- HP VSA configuration, 122
- NetApp SnapMirror configuration, 142

iSCSI LUN/volumes

- EMC Celerra and testing plans,  
292–293
- EMC Celerra replication, 56–63,  
65–71
- error in cleanup phase of Recovery Plan,  
287–288
- NetApp SnapMirror configuration,  
139–141
- testing Recovery Plan, 278

iSCSI Port Binding policy, NetApp  
SnapMirror, 142–143

iSCSI software adapter

- Dell EqualLogic replication, 28–29
- EMC Celerra replication, 53
- HP VSA configuration, 124
- NetApp SnapMirror configuration,  
143–144

upgrading vCenter, 445

iSCSI software initiator

- Dell EqualLogic replication, 26–31
- EMC Celerra replication, 51–56
- HP VSA configuration, 122–127
- NetApp SnapMirror configuration,  
142–147

iSCSI target

- Dell EqualLogic. *See* Dell EqualLogic  
replication
- EMC Celerra replication. *See* EMC  
Celerra replication
- HP VSA configuration, 122–127
- NetApp SnapMirror configuration,  
142–147

ISOs, VR not protecting, 204

## J

---

JVM (Java Virtual Machine) memory,  
vCenter upgrade, 440–441

## K

---

“Keep failback snapshot” option, replicate  
iSCSI volume, 35–36

## L

---

### Licenses

- Celerra iSCSI, 46–47
- facilitate failback process, 399–400
- HP VSA, 104, 113–114
- replication support in storage vendors,  
13–14
- SRA requirements, 194–195
- upgrading vCenter, 436–437
- VMware SRM, 179–180

Linked mode, vCenter, 231, 357–359

- Linked Mode Wizard, 358–359
- Local Reservation, replicate iSCSI volume, 35
- Local storage, HP P4000 VSA, 99
- localSiteStatus node, Advanced Settings dialog box, 361
- Log Out option, from current instance of SRM, 393
- Login
  - configure database for VRMS, 206–207
  - configure pairing process, 229–231
  - configure shared site, 385
  - create EMC LUN, 79
  - create VMware SRM database, 181–182
  - create VSA host, 106–107
  - HIT-VE, 39–40
  - unplanned failover after loss of
    - Protected Site, 416
    - vCenter linked mode, 359
- LUN ID, Create LUN dialog box, 79
- LUN Masks, EMC Celerra and testing plans, 292–293
- LUN number
  - Create LUN dialog box, 79–80
  - grant ESX host access to CLARiiON LUNs, 90–91
- LUNs/volumes
  - allocating snapshots to, 85
  - configure HP VSA for replication, 115–118, 120–122
  - create EMC, 78–80
  - create EqualLogic iSCSI, 23–26
  - create HP VSA, 113–115
  - create multiple datastores, 350–351
  - create NetApp, 134–137, 139–141
  - create reserved LUN pool, 75–78
  - execute Recovery Plan, 401
  - how storage management systems work, 14–18

- HP P4000 VSA, testing at Recovery Site, 127–129
- monitor iSCSI connections, 127
- planned migration with Dell EqualLogic, 404–405
- planned recovery with NetApp a, 405–406
- resignaturing VMFS, 75–78
- scripting recovery test, 425–426
- SRA allowing SRM to discover, 194
- store VMs on multiple datastores, 346–348
- test Recovery Plan after automated failback, 412–413
- test storage configuration at Recovery Site, 273–275
- vendor documentation for, 14
- VMs with raw device/disk mappings and, 348–350
- VMware SRM and, 11

---

## M

- MAC address, licensing VSA with, 99, 104–105
- Managed IP Address
  - deploy VRMS, 210–211
  - set VR installation, 205–206
- Managed object reference (MOREF) number, 334, 339
- Management groups
  - add VSAs to, 108–111
  - configure HP VSA for replication, 114–118
  - set up two VSAs in, 99–100
- Management Groups, Clusters, and Volumes Wizard
  - add VSAs to management console, 108
  - add VSAs to management groups, 108–111

- configure HP VSA for replication, 115–118
  - create cluster, 111–112
  - create volume, 113–114
  - Managing VMware Infrastructure with PowerShell* (Rottenberg), 423
  - Manual DR, 7
  - Manual File Transfer Utility, EqualLogic, 46
  - Mapping Missing error, 336
  - Mappings
    - bidirectional configurations, 376–378
    - configure datastore for VR, 221–222
    - folder, configure Protected Site, 235
    - inventory, configure Protected Site, 231–234
    - network, configure Protected Site, 236–237
    - raw device/disk, 348–350
    - resource, configure Protected Site, 234–235
  - Max Connections, Database Configuration dialog box, 192–193
  - MEM (Multipathing Extension Module), 26
  - Memory
    - HP P4000 VSA requirements, 99
    - reduce RAM in recovery process with PowerCLI, 316–321
    - upgrading vCenter, 440–441
  - Message alarms, 364
  - Message events, Recovery Plan, 282–283
  - Message prompts, Recovery Plan, 310–312
  - Messages, calling scripts within guest OS, 328–329
  - Microsoft
    - Active Directory. *See* Active Directory Sysprep, 4, 329
    - Microsoft SQL Server 2008, configure database for VRMS, 206–208
    - Microsoft SQL Server 2008, VMware SRM database setup
      - configure DSN connection on SRM server(s), 184–185
      - create database and set permissions, 181–184
      - failure to connect to SRM server, 198–199
      - install SRM server, 186–193
      - install storage replication adapter, 193–195
      - install vSphere client SRM plug-in, 195–197
      - overview of, 180–185
    - MirrorView. *See* EMC CLARiiON MirrorView
    - Monitoring, VR, 217–218
    - MOREF (managed object reference)
      - number, 334, 339
    - Move to button, VR, 220
    - msg command, Recovery Plan, 310–311
    - Multipathing Extension Module (MEM), 26
    - Multiple datastores, 346–348, 350
    - Multiple Protection Groups, 351
    - Multiple Recovery Plans, 352–354
- 
- N**
- 
- Naming conventions
    - array manager groups for Dell, 245
    - Celerra file system, 57
    - consistency groups, 88
    - Data Mover interconnect for Celerra replication, 66–67
    - EMC LUN, 79
    - HP VSA cluster, 111
    - HP VSA management groups, 109

Naming conventions, *continued*

- import StorageWorks P4000 VSA, 101
- IQNs for ESX hosts, 29, 54
- iSCSI volumes, 24
- LUNs for reserved LUN pool, 76
- multiple arrays, 256
- NetApp volumes, 138
- Protection Group, 259
- Recovery Plan, 272–273
- remote mirror, 81
- replication schedule, 38
- replication session, 69
- retain original volume name during  
    resignature process, 177–178
- snapshots for SRM tests, 85–87
- vCenter objects, 338–342

## NAT (Network Address Translation)

- IP address changes in recovery VMs  
    using, 330
- IP customization with, 4
- simplify pairing with, 227

## NaviSphere CLI, for EMC VSI, 93

## NetApp FSA

- configure array manager for,  
    254–257
- testing plans and, 294

## NetApp SnapMirror

- configure on Recovery Site, 150–155
- confirm IP visibility and name  
    resolution, 147–148
- create NetApp volumes for Fibre  
    Channel and iSCSI, 139–141
- defined, 147
- enable, 148
- grant ESXi host access, 142–147
- overview of, 131–133
- planned recovery, 405–406
- provision storage for VMware ESXi,  
    133–138

- remote access, 148–150

- Virtual Storage Console, 155–158

## NetApp System Manager

- configure NetApp SnapMirror at  
    Recovery Site, 150–155
- create NetApp volumes, 134–137,  
    139–141
- overview of, 132–133
- save root credentials to prevent endless  
    input, 152

## Network

- communication, VMware SRM  
    architecture, 161–164
- full-site Recovery Plan for, 271–272
- mappings, 232, 236–237
- RAID, 99
- scripting recovery test by fixing VMX  
    files for, 430–431
- scripting site recovery with internal,  
    428–429

Network Address Translation. *See* NAT  
(Network Address Translation)Network TCP/IP Settings, VMware  
Remote Console, 106New Database dialog box, VMware SRM  
database, 181–184New Destination Celerra Network Server,  
Replication Wizard, 65New Login dialog box, Microsoft SQL  
Server 2008, 181–182

## NFS

- create NetApp volume for, 134–137
- grant ESXi host access to NetApp  
    volumes, 137–138
- mount exports when scripting recovery  
    test, 428
- provision NetApp storage for VMware  
    ESXi, 133–138
- test Recovery Plan, 278

## NICs

- bulk changes to IP addresses, 334–335
- enable EMC Celerra iSCSI target on ESX hosts, 51–52, 54
- enable EqualLogic iSCSI target on ESXi hosts, 27
- manual IP guest customization, 330–332

NS-120, 44–45, 73–74

NS-20, 73–74

## O

ODBC Data Source Administrator, configure DSN, 184–185

## Online resources

- EMC VSI plug-in, 94
- execute Recovery Plan with Protected Site, 402
- get started with Celerra VSA, 43
- HP P4000 VSA download, 100
- NetApp ONTAP Simulator, 131
- NetApp VSA, 132
- NetApp VSC, 157
- new SRM plug-in installation, 454
- PowerCLI and PowerShell, 315, 318
- rename and move inventory objects, 338
- virtualize DR, 7
- Virtualizeplanet ReplicaCalc, 165–166
- VMware components, 167
- VMware SRM hardware and software requirements, 170

ONTAP Simulator, NetApp, 131

Organization parameter, shared site configuration, 386

.ovf file, importing HP VSA, 101

## Ownership

- configure database for VRMS, 208
- Microsoft SQL Server 2008, 182–184

## P

P2V (physical to virtual) conversion, 6

## Pairing process

- always configure at Protected Site, 375
- configure VRMS connection, 214–215
- connecting Protected and Recovery Site SRMs, 226–231
- order of configuration, 342
- removing when decommissioning site, 394
- shared site configuration, 392–393

Parameters, pass to command line, 324–325

Partner identification, replication, 32

Partners, configure EqualLogic replication, 32–34

Pass-through authentication, PowerCLI, 322

## Passwords, 33

- configure database for VRMS, 207
- configure DSN on SRM server(s), 185
- configure pairing process, 229, 231
- create EMC LUN, 79
- create VMware SRM database, 181
- deploying VRMS, 210–211
- EMC VSI plug-in, 94
- HIT-VE login, 39–40
- HP VSA management groups, 110
- replication using shared, 33
- run installer for VMware VUM, 443

## Patch process

- ESX host upgrades, 446–448
- VMware Tool upgrade, 457

- Patch update feature, deprecated in VUM, 442–443
- Pause icon, suspend VMs at Recovery Site, 308–309
- Pause option, Recovery Plan test, 286
- Pause Replication button, VR, 220
- Per-physical socket licensing model, SRM, 179
- Per-VM inventory settings, Protection Groups, 264
- Per-VM licensing model, SRM 5.0, 179
- Per-VM mapping, 336–337
- Performance optimization, 348
- Permissions
  - access control, 368–369
  - NetApp volume for NFS, 135–136
  - real execution of Recovery Plan, 399
  - SRM administrators delegation, 371–372
  - VMware SRM database, 181–184
- Physical couriering, replication for, 220–221
- Physical servers, in DR plan, 5–7
- Physical to virtual (P2V) conversion, 6
- ping test
  - Dell EqualLogic replication, 27
  - EMC Celerra replication, 52, 64
  - HP VSA configuration, 103, 123
  - NetApp SnapMirror configuration, 142–143, 147–148
- Placeholder datastores
  - configure database for VRMS, 206–208
  - configure Protected Site, 238–241
  - Recovery Site configuration errors and, 290
  - reprotect process requiring, 407–409
  - test storage configuration at Recovery Site, 274, 279
- Placeholder VMs
  - accidental deletion error, 264–265
  - configure Protection Groups, 260–262
- Protection Groups determining location of, 225
- Recovery Site configuration errors and, 290
- redirect process creating, 410–411
- test Recovery Plan, 279
- VMware Tool upgrade, 456
- Planned migration
  - automated failback from, 407–415
  - Dell EqualLogic and, 404–405
  - execute Recovery Plan with Protected Site, 402–404
  - NetApp and, 405–406
  - Recovery Steps mode vs. test step, 398
  - test Recovery Plan with, 413
  - when Protected and Recovery sites are connected, 417–418
- Plug-in Manager
  - upgrading SRM 4.1 to 5.0, 454
  - upgrading VUM plug-in, 443–445
- Policies, PowerCLI, 315
- Port binding, iSCSI, 27–28, 51–53
- Port groups
  - configuration and identifiers held by ESX hosts, 339
  - create internal network for scripting recovery test, 428–429
  - deploy VRMS, 209–210
  - rename in Protected Site, 339–341
  - rename in Recovery Site, 342
  - select for VSA, 103
  - set ephemeral ports in vCenter upgrade, 441
  - test Recovery Plan, 280
- Post Power On Steps, Recovery Plan, 310–311
- Power on VMs
  - add VM dependencies, 302–305
  - configure custom Recovery Plan for how to, 299

- configure priorities for recovered VMs, 299–302
- configure start-up and shutdown options, 305–307
- disabling, 381–384
- Pre-power On Step, 310–311, 324
- PowerCLI
  - add command steps, 315–321
  - control start-up orders with vApps, 383
  - manage authentication and variables, 321–327
  - overview of, 315–316
  - reduce RAM used in recovery process, 316–321
  - scripting site recovery. *See* Scripting site recovery for test
- Powered-off VMs
  - errors after unplanned failover from loss of Protected Site, 417
  - execute Recovery Plan with Protected Site, 402–404
  - not replicated by VR, 204
  - virtual hardware upgrade, 458–459
- PowerShell, command steps, 315–321
- A Practical Guide to Business Continuity & Disaster Recovery with VMware Infrastructure*, 7
- Pre-power-on scripts, PowerCLI, 321
- Pre-power On Step, VMs, 310–311, 324
- Presynchronize storage, Recovery Steps mode, 399
- Priorities
  - configure for recovered VMs, 299–302
  - configure VM dependencies, 302–305
  - levels of, 4
- Privileges, PowerCLI pass-through authentication, 322–323
- Product limitations, VMware SRM, 178–179
- Production systems, virtualizing for DR, 5–7
- Prompt steps, Recovery Plans, 309–312
- Properties
  - after upgrading VMFS, 461
  - ESX host access to HP VSA iSCSI target, 124–125
  - ESXi host access to NetApp iSCSI target, 144
  - iSCSI Initiator, 29–30
- Protected Site
  - automated failback from planned migration, 407–415
  - Celerra replication configuration. *See* EMC Celerra replication
  - create/enable alarm for new VM, 362–363
  - decommissioning, 394
  - EMC CLARiiON MirrorView replication, 91–93
  - EMC MirrorView configuration, 80–85
  - EqualLogic replication at, 35–36
  - execute Recovery Plan with available, 400–404
  - failback. *See* failback
  - failover. *See* failover
  - goal of VMware SRM, 10–11
  - HIT-VE configuration, 41
  - NetApp SnapMirror configuration, 148–150
  - network communication and TCP port numbers, 161–164
  - pairing sites together, 392–393
  - planned migration with Dell EqualLogic, 404–405
  - planned migration with NetApp, 405–406
  - PowerCLI install, 315
  - shared site configuration, 387–390



**Protected Site, *continued***

- SRM administrators delegation, 371
  - SRM server connectivity failures, 198–199
  - SRM software install, 186
  - SRM tasks carried out at, 375
  - storage replication components, 164–166
  - synchronous replication limitations, 13
  - unplanned failover after total loss of, 415–419
  - upgrading vSphere at, 436
  - VMware components, 167–169
  - VR technology structure, 203
- Protected Site configuration**
- array managers, DellEquaLogic, 245–248
  - array managers, EMC Celerra, 248–251
  - array managers, EMC CLARiiON, 251–254
  - array managers, introduction, 241–245
  - array managers, NetApp FSA, 254–257
  - assigning placeholder datastores, 237–241
  - connecting Protected and Recovery Site SRMs, 226–231
  - failure to protect virtual machine, 262–266
  - folder mappings, 235
  - inventory mappings, 231–234
  - network mappings, 236–237
  - overview of, 225
  - Protection Groups, 257–262
  - resource mappings, 234–235
  - summary review, 267–268
  - VRMS, 212–214
- Protected Site, managing changes at**
- create and protect new VMs, 337–338
  - other objects and changes, 342–343
  - overview of, 337

- rename and move vCenter inventory objects, 338–342
  - Storage vMotion and Protection Groups, 343–346
  - VMs stored on multiple datastores, 346–348
  - VMs with raw device/disk mappings, 348–350
- Protection Groups**
- assign placeholder datastores for, 237–239
  - configure for Protected Site, 257–262
  - created for bidirectional configuration, 380
  - customize VM mappings with, 336
  - deletion of, 262
  - enroll new VMs in, 337–338
  - failure to protect, 262–266
  - indicating VMs utilizing multiple datastores, 346–347
  - inventory mappings and, 232
  - license for, 180
  - loss of settings after Recovery Plan test, 288–289
  - move VMFS to new system with Storage vMotion, 461–462
  - multiple, 351
  - order of configuration of SRM, 343
  - overview of, 18–19
  - remove when decommissioning site, 394
  - select for Recovery Plan, 270–271
  - Storage vMotion and, 343–346
- Protection node, source NetApp filer, 151**
- Protocol-neutral, VR as, 3**
- Provisioning and Cloning tab, NetApp VSC, 156–158**
- Provisioning storage**
- EMC VSI, 94
  - NetApp NFS for VMware ESXi, 133–138
  - .ps files, 316–321

## Q

Qtree Details page, Create Mirror Wizard, 152

## R

### RAID groups

defined, 78

EMC CLARiiON, 44

EMC LUN, 78–80

LUNs for reserved LUN pool, 76

RAM, reduce in recovery process, 316–321

Rate of Change Rule of Thumb (RCRT), 165–166

Raw device/disk mappings (RDMs), 204, 348–350

RCRT (Rate of Change Rule of Thumb), 165–166

RDMs (raw device/disk mappings), 204, 348–350

Re-IP process, improved in SRM 5.0, 4–5

### Reboot

change in ESX iSCSI stack, 31, 56

ESXi host access to NetApp iSCSI target, 146

HIT-VE configuration, 40–41

virtual hardware upgrade, 459

VMware Tool upgrade, 457

VMware Update Manager, 442

Reciprocity, pairing process, 227

RecoverPoint technology, EMC, 119

Recovery button, 399, 402

### Recovery Plans

basic full-site, 269–273

bidirectional configurations, 381

clean up after test, 283–285

control and troubleshoot, 285–291

create, 262–266

disable power-on function of VMs, 383

order of configuration of SRM, 343

pause, resume and cancel, 285–287

remove when decommissioning site, 394

reprotect process. *See* Reprotect process

run after unplanned failover from loss of Protected Site, 415–417

run multiple simultaneous, 276

SRM 5.0 protection for, 10

storage array vendors and, 291–294

test, basic steps, 277–281

test, exercise, 281–283

test storage configuration, 273–275

test, understanding, 275–276

test with Protection Groups, 257–262

view Recovery Steps, 397–398

### Recovery Plans, custom

add command steps, 313–314

add command steps with VMware PowerCLI, 315–321

add prompt steps, 309–312

add VM dependencies, 302–305

configure IP address changes for Recovery VMs, 329–337

configure priorities for recovered VMs, 299–302

configure start-up and shutdown options, 305–307

control how VMs power on, 299

lost Repair Array Managers button, 354

manage changes at Protected Site. *See* Protected Site, managing changes at

manage PowerCLI authentication and variables, 321–327

multiple datastores, 350–351

multiple Protection Groups, 351

multiple Recovery Plans, 352–354

overview of, 297–298

review summary, 354–355

suspend VMs at Recovery Site, 308–309

- Recovery point objectives. *See* RPOs (recovery point objectives)
- Recovery Profile Prompt Display alarm, 364
- Recovery Site
  - automatic resignature of volumes in, 177
  - configure HIT-VE at, 41
  - connect SRMs for both Protected Site and, 226–231
  - create/enable alarm for new VM, 362–363
  - create SRM administrators delegation, 371
  - decommissioning, 394
  - enable EMC Celerra replication at, 56, 58–59, 63–71
  - enable EMC CLARiiON MirrorView at, 81–84, 90–91
  - enable EqualLogic replication, 35–36
  - enable EqualLogic replication at, 30
  - enable HP P4000 VSA at, 127–129
  - enable NetApp SnapMirror at, 137, 148–155
  - goal of VMware SRM, 10–11
  - installing SRM software, 186
  - license VMware SRM at, 179
  - managing changes at, 342
  - network communication and TCP port numbers, 161–164
  - pairing sites together, 392–393
  - Recovery Plans carried out at. *See* Recovery Plans
  - shared site configuration, 390–391
  - SRM server connectivity failures, 198–199
  - storage replication components, 164–166
  - suspend VMs at, 308–309
  - synchronous replication limitations, 13
    - unplanned failover after total loss of Protected Site, 415–419
    - VMware components, 167–169
    - VR technology structure, 203
- Recovery Site configuration
  - clean up after Recovery Plan test, 283–285
  - create basic full-site Recovery Plan, 269–273
  - first Recovery Plan test, 275–281
  - first Recovery Plan test, exercise, 281–283
  - pause, resume and cancel Recovery Plan, 285–287
  - Recovery Plans and storage array vendors, 291–294
  - test storage configuration, 273–275
- Recovery Site configuration, errors
  - clean up after Recovery Plan test, 287–288
  - disconnected hosts at Recovery Site, 290–291
  - loss of Protection Group settings, 288–289
  - repairing VMs, 290
  - use force cleanup when cleanup fails, 289–290
- Recovery Steps tab, Recovery Plan, 301, 304–305, 397–398
- redirect.cmd file, 318
- Refresh array manager, bidirectional configuration, 378–379
- Registration
  - add VMs to inventory for scripting recovery test, 429–430
  - assign placeholder datastores, 238
  - bad inventory mappings from failure of, 262–264
  - run installer for VMware VUM, 443
  - upgrading SRM 4.1 to 5.0, 452

- Relationships
  - Celerra replication, 65–66
  - replication partners, 32–34
  - VM Dependencies showing VM, 4
- Release notes, VMware SRM product
  - limitations, 178–179
- Reload SRAs link, Array Manager pane, 242
- Remediation process, upgrading ESX hosts, 448–449
- Remediation Selection Wizard, 448–450
- Remote access, NetApp SnapMirror, 148–150
- Remote Replicas view, 37
- Remote Reservation, replication of iSCSI volume, 35
- Remote Setup Wizard, 23
- remote-signed policy, PowerCLI install, 315
- Remove Replication button, VR, 220
- Renouf, Alan, 315, 318–321, 423
- Repair Array Managers button (deprecated), 354
- Replicas icon, 86–89
- Replication
  - configure HP VSA for, 114–118
  - configure vSphere. *See* VR (vSphere Replication)
  - configure with EqualLogic. *See* Dell EqualLogic replication
  - configure with NetApp storage. *See* NetApp SnapMirror
  - EMC Celerra. *See* EMC Celerra replication
  - with EMC CLARiiON. *See* EMC CLARiiON MirrorView
  - execute Recovery Plan at Protected Site with Dell EqualLogic, 398–399
  - execute Recovery Plan with Protected Site, 400–402
  - how storage management systems work, 14–18
  - monitor HP VSA, 118–119
  - principles of, 12–14
  - reprotect process reversing direction of, 408–410
  - unplanned failover after loss of Protected Site, 416–417
  - VMware SRM and, 11
  - VMware SRM components for, 164–166
  - vSphere. *See* VR (vSphere Replication)
- Replication Wizard, Celerra replication, 64–71
- Replications tab, Replication Wizard, 70–71
- Reprotect process
  - cleanup after, 414–415
  - new in SRM 5.0, 3
  - overview of, 407–409
  - test Recovery Plan, 412–415
  - triggering, 409–412
- Rescans of ESX hosts, scripting site recovery, 426–427
- Reserved LUN pool (RLP), 75–78, 86
- Resignature VMFS volumes
  - scripting recovery test, 427–428
  - VMware SRM, 173–178
- Resource mappings
  - bidirectional configuration, 376–377
  - configure Protected Site, 234–235
  - defined, 234
- Resource pools
  - configure resource mappings, 234–235
  - rename in Protected Site, 339
  - rename in Recovery Site, 342
  - select for VSA, 102
- Resources, run multiple Recovery Plans simultaneously, 276
- Restore All link, Placeholder Group, 264–265
- Restore Placeholder link, Placeholder Group, 264–265
- Resume option, Recovery Plan test, 286

Resume Replication button, VR, 220  
RLP (reserved LUN pool), 75–78, 86  
Roles

- automatic replication of group, 370
- SRM administrators delegation, 370–372
- SRM network communication, 161–162
- vCenter access control, 369–370

Root credentials, 328  
Rottenberg, Hal, 423  
RPOs (recovery point objectives)

- calculate bandwidth to meet, 165
- configure Celerra replication, 69–70
- create schedule for replication that meets, 37–39

RTOOLS software, EMC VSI

- requirement, 93

RTOs (recovery time objectives),

- replication schedule based on, 37–39

## S

---

Scalability

- for the cloud, 9–10
- of VMware SRM, 171–172

Schedule, replication

- bandwidth determining frequency of, 165
- EqualLogic, 37–39
- managing from vCenter, 40–41
- NetApp SnapMirror at Recovery Site, 153–155

Scripting site recovery for test

- add VMs to inventory, 429–430
- create internal network for test, 428–429
- fix VMX files for network, 430–432
- manage storage, 425–426
- mount NFS exports, 428
- overview of, 423–425
- rescan ESX hosts, 426–427
- resignature VMFS volumes, 427–428
- using SRM vs., 423–424, 432

Scripts

- add command steps to call within guest OS, 328–329
- alarm, 362–363
- configure multiple VSAs, 100
- PowerCLI authentication in Recovery Plan, 324–325
- PowerCLI variables in Recovery Plan, 325–327

SDK (Software Development Kit),

- automating SRM, 191

Secondary image LUN

- create snapshot for SRM tests, 85–88
- for EMC MirrorView, 81–84

Security

- create VMware SRM database, 181
- install SRM software, 189–190
- install vSphere client SRM plug-in, 196–197

Security Profile, 143  
Select Database Owner dialog box, 182–184  
Send Email option, SRM service alarm, 364–365  
Senior management, approval of real execution of Recovery Plan, 397–399  
Server software, upgrading vCenter, 440  
Service alarm, 364–365  
Service Console, resignature VMFS volumes, 427  
Service dependencies, configure VM power on, 299  
Services MMC, resuming Recovery Plan test, 286  
set-vm cmdlet, 316, 318  
Shadow VMs, 408, 410–411  
Shanklin, Carter, 423

- Shared site configurations
  - decommissioning site, 394
  - install SRM with custom options to new site, 387–390
  - install SRM with custom options to Recovery site, 390–391
  - overview of, 384–387
  - pairing sites together, 392–393
- Shut-down options, control in Recovery Plan, 305–307
- Site pairing. *See* Pairing process
- Site Recovery Adapter. *See* SRA (Site Recovery Adapter)
- Site Recovery icon, 270
- Site Recovery Manager. *See* SRM (Site Recovery Manager)
- Site Recovery Manager vSphere Replication, 217–218
- Size, iSCSI volume, 24–25
- SMB market, VR for, 2–3
- SnapMirror. *See* NetApp SnapMirror
- Snapshots
  - allocation of space for, 24–25
  - configure HP VSA for replication, 115–118
  - create for SRM tests, 85–88
  - Dell EqualLogic and testing plans, 291–292
  - determining replication frequency, 165
  - EMC Celerra and testing plans, 292–293
  - enable EMC Celerra replication, 58–59
  - execute Recovery Plan with Protected Site, 400–401
  - grant ESX host access to CLARiiON LUNs, 92–93
  - iSCSI error in cleanup phase of Recovery Plan, 287–288
  - monitor HP VSA replication, 118–119
  - NetApp and testing plans, 294
  - reserved LUN pool for all, 75
  - resignature VMFS volumes, 175–176
  - test Recovery Plan, 278–280
  - upgrading SRM to 5.0, 451
  - VMware SRM and, 11
  - VR not protecting, 204
- SOAP listener port, 191
- Software
  - installing SRM, 186–193
  - VMware SRM requirements, 169–171
- Software Development Kit (SDK), automating SRM, 191
- Source, Replication Wizard, 69
- Space page, create iSCSI volume, 24–25
- Specify Destination Celerra Network Server, Replication Wizard, 65
- Spoke and hub configuration, shared sites, 384
- SQL Authentication
  - for SQL Server database, 180
  - Update Manager only supporting, 443–444
  - upgrading vCenter with, 440
- SQL Management Studio, 180–181
- SRA (Site Recovery Adapter)
  - array manager configuration, 242–244
  - automated failback via, 3
  - configure SRM array manager, 163–164
  - at Recovery Site, 11
- SRA (Storage Replication Adapter), 193–195
- SRM array manager, configure, 163–164
- SRM Extension ID, SRM, 385
- SRM ID parameter
  - pairing sites together, 392–393
  - shared site configuration, 385–386, 387–391
- SRM installer, 384–391
- srm-migrate command, upgrade to 5.0, 454–455

- SRM (Site Recovery Manager)
  - access control, 369–370
  - configure VRMS from UI extensions, 212–214
  - create administrator, 370–371
  - deploy VRMS from UI extensions, 208–211
  - failure while testing Recovery Plan, 286–287
  - install vSphere client plug-in, 196–197
- SRM (Site Recovery Manager) 5.0
  - introduction
  - automated failback and reprotect, 3
  - file level consistency, 11–12
  - history before, 5–7
  - how most storage systems work, 14–16
  - IP customization improved, 4–5
  - storage management and replication
    - principles, 12–14
  - storage planning considerations, 16–19
  - understanding, 10–11
  - upgrading to. *See* Upgrading SRM 4.1 to 5.0
  - VM Dependencies, 4
  - vSphere 5 compatibility, 2
  - vSphere Replication, 2–3
  - what is not DR technology, 7–10
- Stage process, upgrade ESX hosts, 448–449
- Standard vSwitches. *See* SvSwitches (Standard vSwitches)
- start-sleep command, PowerCLI, 383
- Start-up options, control in Recovery Plan, 305–307
- Start-up orders, vApp, 381–384
- Start-vApp cmdlet, PowerCLI, 383
- Status, Recovery Plan, 282
- Storage configuration
  - Recovery Site tests, 273–275
  - upgrading SRM 4.1 to 5.0, 452–453
- Storage load balancing, EqualLogic, 24
- Storage management
  - file level consistency and, 11–12
  - principles of, 12–14
  - scripting site recovery, 425–426
  - understanding SRM, 10–11
- Storage Pool, 56–57
- Storage Replication Adapter (SRA), 193–195
- Storage replication components, 164–166
- Storage vMotion, 343–346, 461–462
- StorageWorks P4000 VSA. *See* HP StorageWorks P4000 VSA (virtual storage appliance)
- Stretched clusters, 8–9, 165
- Stretched VLANs, 226, 236–237
- Successes, testing Recovery Plan, 277
- Summary page, replication of iSCSI volume, 46
- Suspend VMs at Recovery Site, 308–309
- SvSwitches (Standard vSwitches)
  - bad inventory mappings from, 264
  - create full-site Recovery Plan, 271
  - enable EMC Celerra iSCSI target on ESX hosts, 51–52
  - enable EqualLogic iSCSI target on ESXi hosts, 27
  - grant ESX host access to HP VSA iSCSI target, 123
  - grant ESXi host access to NetApp iSCSI target, 142–143
  - map between DvSwitches and, 237
  - rename virtual port groups in Protected Site, 339–340
  - scripting recovery test, 430–431
  - select network port group for VSA on, 103
  - test Recovery Plan, 280
- Synchronization rate, configure EMC MirrorView, 83–85

Synchronize Now button, VR, 220  
 Synchronize Storage process, test Recovery Plan, 277–278  
 Synchronous replication  
   configure HP VSA for, 118–119  
   create EMC LUN, 78–79  
   limitations of, 13  
   reprotect process, 409–410  
   unplanned failover after loss of Protected Site, 417

## T

Target Wizard, 48–50  
 Tasks, configure Protection Groups, 259–260  
 TCP port 3260  
   ESXi opening automatically, 53  
   grant ESX host access to HP VSA iSCSI target, 123–124  
   grant ESXi host access to NetApp iSCSI target, 143–144  
 TCP port numbers, SRM architecture, 161–164  
 Templates  
   bad inventory mappings from, 264  
   protect on replicated datastore, 261  
   save replication schedules as, 39  
 Terminology, varying between storage vendors, 12–13  
 Test Networks dialog box, full-site Recovery Plan, 271–272  
 Tests  
   first Recovery Plan, 275–281  
   first Recovery Plan, exercise, 281–283  
   real execution of Recovery Plan vs., 397–398  
   scripting site recovery for. *See* Scripting site recovery for test

  storage configuration at Recovery Site, 273–275  
   understanding, 275–276  
 Thinly provisioned volumes, 25, 113–114  
 Third-party plug-ins, upgrading, 445  
 3Par's SRA, 194  
 Thumbprint, certificates, 188–189  
 Times, replication schedule, 38  
 Trap Retriever, 364–365  
 Troubleshooting, Recovery Plans, 285–291  
 Trust, Celerra replication, 65–66  
 Trusted certificates, SRM software install, 188–189

## U

UI extensions, VRMS deployment from, 208–211  
 Underscore (\_) HP VSA management group names, 109  
   VM names during reprotect process, 407–408  
 Unidirectional configuration, 164, 179  
 Unisphere management system  
   add systems to, 45–46  
   Celerra licensing for iSCSI, 46–47  
   create EMC Celerra iSCSI target, 48  
   create EMC LUN, 79–80  
   create LUNs for reserved LUN pool, 76–78  
   create new Celerra file system, 56–59  
   create snapshot for SRM tests, 86  
   defined, 44  
   EMC Celerra and testing plans, 292–293  
   EMC VSI requirement, 93  
   grant ESX host access to CLARiON LUNs, 90–93



Unisphere management system, *continued*  
overview of, 73–74  
ping tests for IP communication between  
two arrays, 64

Unplanned failover  
cleanup after, 414–415  
when Protected Site is dead, 415–419

Update Manager, and VMware Tools  
update error, 265–266

Update Policy, Celerra replication,  
69–70

Update Tools, PowerCLI, 457

Upgrade checker utility, 436–437

Upgrading SRM 4.1 to 5.0  
DvSwitches, 462  
overview of, 433–435  
SRM, 452–455  
upgrading vSphere. *See* Upgrading  
vSphere 4 to vSphere 5  
virtual hardware, 458–460  
VMFS volumes, 460–462  
VMware Tools, 455–457

Upgrading vSphere 4 to vSphere 5  
client, 441–442  
ESX hosts, 445–451  
overview of, 435–436  
run upgrade checker, 436  
third-party plug-ins, 445  
vCenter, 436–441  
VUM, 442–443  
VUM plug-in, 443–445

User account, for vCenter upgrade, 436

Username  
configure database for VRMS, 207  
configure DSN on SRM server(s), 185  
configure pairing process, 229, 231  
create EMC LUN, 79  
create VMware SRM database, 181  
HIT-VE login, 39–40

HP VSA management groups, 110  
run installer for VMware VUM, 443  
use EMC VSI plug-in, 94

UUID value, resignaturing VMFS  
volumes, 174–178

---

## V

Van Zantan, Gabriele, 425, 429

vApps  
bidirectional configuration with,  
376–378  
configure inventory mappings with,  
376–378  
control start-up orders with, 381–383  
registration of VRS requiring, 216  
upgrading vCenter, 441

Variables, PowerCLI, 321–327

vCenter  
client, upgrading to vSphere 5, 441–442  
clone VSAs with, 99  
configure HIT-VE for, 39–40  
connection failure after unplanned  
failover of Protected Site,  
415–416  
create alarm script, 362–363  
linked mode, 357–358, 394  
rename and move inventory objects in,  
338–342  
rescan ESX hosts in, 426–427  
roles, 369–370  
schedules managed directly from, 40–41  
set Managed IP Address for VR  
installation, 205–206  
SRM software install, 186–187  
upgrading, 436–441  
VMware SRM communication role,  
162–164

- vCLI, resignation of VMFS volumes, 427
- vCloud Director, VMware, 10, 440–441
- Vendors, storage array
  - all systems are the same, 12–13
  - array manager configuration for. *See* array manager configuration
  - documentation of, 14
  - how storage management systems work, 14–16
  - real execution of Recovery Plan and, 399
  - Recovery Plans and, 291–294
  - replication support differences in, 13–14
  - scripting recovery test and, 425–426
  - test storage configuration at Recovery Site, 274
  - upgrading to SRM 5.0, 452–453
- vicfg-volume command, 427
- View component
  - new in SRM 5.0, 298
  - Recovery Plan history, 367–368
- Virtual disks
  - add to HP P4000 VSA, 104
  - enable replication for physical couriering, 220–221
  - enable vSphere Replication, 218–219
  - select format for HP P4000 VSA, 103
  - store VMs on multiple datastores, 346–348
- Virtual hardware, upgrading, 458–460
- Virtual IPs, clusters for HP VSA, 111–112
- Virtual iSCSI HBA, monitor iSCSI connections, 127
- Virtual Machines tab, Recovery Plan, 381, 458–459
  - add per-VM messages, 310–311
  - add VM dependencies, 304–305
  - change power-on state of VMs, 307
- virtual storage appliance (VSA)
  - HP P4000. *See* HP StorageWorks P4000 VSA (virtual storage appliance)
  - NetApp. *See* NetApp SnapMirror
- Virtual Storage Console (VSC), 133, 155–158
- Virtual Storage Integrator (VSI) plug-in, EMC, 93–95
- Virtualization, before VMware SRM, 5–7
- VM Dependencies
  - add to Recovery Plan, 302–305
  - configure priorities for recovered VMs, 300
  - configure start-up/shutdown options, 306
  - new in SRM 5.0, 4
- VM ID, configure bulk changes to IP, 333–334
- VMDK, 346–348
- VMFS extents
  - how storage management systems work, 16–17
  - replicate all LUNs using, 18
  - as temporary band-aid in short term, 17–18
  - VMware SRM and, 11
- VMFS (VMware File System) volumes
  - clean up after, 414–415
  - format iSCSI LUN with, 63
  - manage storage when scripting recovery test, 425–426
  - resignating, 173–178
  - resignating when scripting recovery test, 427–428
  - store HP P4000 VSA on local vs. shared, 99
  - store RDM mapping file on, 349
  - upgrade to SRM 5.0, 460–462

## VMFS volumes

- Dell EqualLogic and testing plans, 291–292
- EMC Celerra and testing plans, 292–293
- testing Recovery Plan, 278–279

## VMkernel port group

- enable EMC Celerra replication, 51–56
- enable EqualLogic replication, 26–27
- enable HP VSA configuration, 122–126
- enable NetApp SnapMirror, 136–138, 142–145

## vmkping

- enable EMC Celerra replication, 52
- enable EqualLogic replication, 27
- enable HP VSA configuration, 103, 123
- enable NetApp SnapMirror, 142–143

## vMotion, 7–8

## VMs (virtual machines)

- add to inventory for scripting recovery test, 429–430
- create alarm script for new, 362–363
- rename in Protected Site, 339
- SRM 5.0 protection for, 10
- upgrading virtual hardware, 458–459

## vmware-cmd, 429

## VMware Converter, 6

VMware File System. *See* VMFS (VMware File System) volumesVMware PowerCLI. *See* PowerCLI

## VMware Remote Console window, 105–107

## VMware SRM architecture

- configure VMware components, 166–169
- failover and failback design, 172–173
- hardware and software requirements, 169–171
- licensing, 179–180
- network communication and TCP port numbers, 161–164

## overview, 161

- product limitations, 178–179
- resignaturing VMFS volumes, 173–178
- scalability of VMware SRM, 171–172
- storage replication components, 164–166

VMware SRM installation. *See also* VMware SRM architecture

- configure DSN connection on SRM server(s), 184–185
- create database and setting permissions, 181–184
- failure to connect to SRM server, 198–199
- install SRM server, 186–193
- install storage replication adapter, 193–195
- install vSphere client SRM plug-in, 195–197
- ISRM installation, database setup, 180–185

## VMware Tools

- call scripts within guest OS in PowerCLI and, 328
- create manual IP guest customization, 330–332
- heartbeat service, 282, 306
- update error, Protection Groups, 265–266
- upgrade SRM to 5.0, 455–457

VMware Update Manager. *See* VUM (VMware Update Manager)

*VMware vSphere PowerCLI Reference: Automating vSphere Administration*, 423

*VMware vSphere PowerCLI Reference: Automating vSphere Administration* (Renouf, Dekens et al.), 423

- VMX files
  - assign placeholder datastores, 238–241
  - automatic resignature of volumes in Recovery Site, 177
  - configure Protection Groups, 260–261
  - scripting recovery test, 430–431
  - test Recovery Plan, 280
- Volume Activities pane, 34
- Volume replica, 46
- Volume Settings page, iSCSI volume, 24
- Volume Shadow Copy Service (VSS), enabling VR, 218
- Volumes. *See* LUNs/volumes
- VR (vSphere Replication)
  - configure datastore mappings, 221–222
  - create Recovery Plan for, 271
  - deploying VRMS, 208–211
  - enable and monitor, 217–219
  - enable for physical couriering, 220–221
  - forced synchronization, 220
  - how it works, 201–202
  - install SRM software, 186–187
  - limitations of, 203–204
  - move, pause, resume and remove, 220
  - new in SRM 5.0, 2–3
  - objects and changes in, 342–343
  - overview of, 201–202
  - registering VRS, 216–217
  - scalability limits, 172
  - StorageVMotion not impacting configurations, 343
  - structure of technology, 203
- VRA (vSphere Replication agent), 203
- VRMS (vSphere Replication Management Server)
  - configure, 212–214
  - configure connection, 214–215
  - configure database for, 206–208
  - deploying, 208–211
  - VR technology structure, 203
- VRS (vSphere Replication server)
  - deployment, 215
  - enable vSphere Replication, 219–220
  - register, 216–217
  - VR technology structure, 203
- VSA (virtual storage appliance)
  - HP P4000. *See* HP StorageWorks P4000 VSA (virtual storage appliance)
  - NetApp. *See* NetApp SnapMirror
- VSC (Virtual Storage Console), 133, 155–158
- VSI (Virtual Storage Integrator) plug-in, EMC, 93–95
- vSphere
  - client SRM plug-in installation, 195–197
  - components not protected by VR, 204
  - Replication tab, 208, 212, 214
  - SRM 5.0 compatibility with, 2
- vSphere 4 to vSphere 5 upgrade path
  - ESX hosts, 445–451
  - overview of, 435–436
  - run upgrade checker, 436
  - third-party plug-ins, 445
- vCenter, 436–441
- vCenter client, 441–442
- VUM, 442–443
- VUM plug-in, 443–445
- vSphere Replication. *See* VR (vSphere Replication)
- vSphere Replication agent (VRA), 203
- vSphere Replication Management Server. *See* VRMS (vSphere Replication Management Server)
- vSphere Replication server. *See* VRS (vSphere Replication server)

- VSS (Volume Shadow Copy Service),
  - enabling VR, 218
- vSwitch
  - enable EMC Celerra replication, 51–52
  - enable EqualLogic replication, 26–27
  - select network port group for VSA on, 103
  - test Recovery Plan, 280–281
- VUM (VMware Update Manager)
  - upgrading, 442–443
  - upgrading ESX hosts, 444–451
  - upgrading plug-in, 443–445
  - upgrading virtual hardware, 459–460
  - upgrading VMware Tools, 456–457

---

## W

- Warnings
  - array manager configuration, 242
  - installer for VMware VUM, 443
  - upgrading vCenter database, 437–439
- WILs (write intent logs), reserved LUN pools, 75–78

---

## Y

- Yellow exclamation point, Protection Group, 266

PEARSON

**InformIT** is a brand of Pearson and the online presence for the world's leading technology publishers. It's your source for reliable and qualified content and knowledge, providing access to the top brands, authors, and contributors from the tech community.

↕ Addison-Wesley

Cisco Press

EXAM/CRAM

IBM Press

QUE

PRENTICE HALL

SAMS

Safari

## LearnIT at InformIT

Looking for a book, eBook, or training video on a new technology? Seeking timely and relevant information and tutorials? Looking for expert opinions, advice, and tips? **InformIT has the solution.**

- Learn about new releases and special promotions by subscribing to a wide variety of newsletters. Visit **informit.com/newsletters**.
- Access FREE podcasts from experts at **informit.com/podcasts**.
- Read the latest author articles and sample chapters at **informit.com/articles**.
- Access thousands of books and videos in the Safari Books Online digital library at **safari.informit.com**.
- Get tips from expert blogs at **informit.com/blogs**.

Visit **informit.com/learn** to discover all the ways you can access the hottest technology content.

### Are You Part of the IT Crowd?

Connect with Pearson authors and editors via RSS feeds, Facebook, Twitter, YouTube, and more! Visit **informit.com/socialconnect**.



# Try Safari Books Online FREE

Get online access to 5,000+ Books and Videos



**Safari**<sup>®</sup>  
Books Online

**FREE TRIAL—GET STARTED TODAY!**  
[www.informit.com/safaritrial](http://www.informit.com/safaritrial)

## ➤ Find trusted answers, fast

Only Safari lets you search across thousands of best-selling books from the top technology publishers, including Addison-Wesley Professional, Cisco Press, O'Reilly, Prentice Hall, Que, and Sams.

## ➤ Master the latest tools and techniques

In addition to gaining access to an incredible inventory of technical books, Safari's extensive collection of video tutorials lets you learn from the leading video training experts.

## WAIT, THERE'S MORE!

## ➤ Keep your competitive edge

With Rough Cuts, get access to the developing manuscript and be among the first to learn the newest technologies.

## ➤ Stay current with emerging technologies

Short Cuts and Quick Reference Sheets are short, concise, focused content created to get you up-to-speed quickly on new and cutting-edge technologies.

Addison  
Wesley

Adobe Press

ALPHA

Cisco Press

FT Press  
FINANCIAL TIMES

IBM  
Press

lynda.com

Microsoft  
Press

New  
Riders

O'REILLY

Peachpit  
Press

PRENTICE  
HALL

que

Redbooks

SAMS

SAS  
Publishing

Sun  
microsystems

WILEY-INTERSCIENCE  
Publishing

WILEY