

WHITE PAPER

Disaster Recovery for FUJIFILM Medical Systems Synapse® Portfolio with VMware® Site Recovery Manager



FUJIFILM Medical Systems USA, Inc.
Thomas E. Riddle and Ray Milot

FUJIFILM



Contents

- Introduction..... 1**
- Components2**
 - VMware Site Recovery Manager.....2
 - Third Party SAN Storage and Data Replication.....3
 - Fujifilm Synapse® Overview.....3
- Solution Design and Setup5**
 - Architecture5
 - Software Used7
 - Hardware and Software Configuration9
 - Site Recovery Manager Installation and Configuration.....9
 - Primary and Secondary site:.....9
 - Primary Site:.....10
 - Secondary Site:10
- Disaster Recovery Testing..... 12**
 - Execute Recovery Plan Test.....12
 - Execute Recovery Plan Actual.....15
- Conclusion 17**
- Appendix A: Site Recovery Manager Setup..... 18**
 - Configure Storage Array Manager (Primary Site)18
 - Configure Inventory mappings (Primary Site)19
 - Create Protection Group (Primary Site).....19
 - Create Recovery Plan (Secondary Site).....22
- Appendix B: References..... 25**
 - VMware:.....25
 - FUJIFILM:25

Introduction

This document outlines how you can benefit from a virtualized, multi-tier Synapse® environment from FUJIFILM Medical Systems USA (Fujifilm) that is configured with VMware® Site Recovery Manager. Learn how you can:

- Accelerate recovery for the virtual environment through automation.
- Ensure reliable recovery by enabling non-disruptive testing.
- Simplify recovery by eliminating complex manual recovery steps and centralizing management of recovery plans.

Healthcare organizations that have deployed Fujifilm's Synapse applications depend heavily on the information, processes and availability of the environment, even in the case of a disaster. However, the complexity and distributed nature of these applications can make implementation and maintenance of traditional disaster recovery solutions expensive and complicated.

VMware virtualization technology helps overcome the challenge of achieving cost effective disaster recovery. This paper introduces an approach to disaster recovery that uses VMware Site Recovery Manager and block-based SAN storage replication to provide an effective availability solution for mission-critical Fujifilm Synapse deployments.

This paper documents a small-scale lab validation that demonstrates the key concepts of VMware Site Recovery Manager (SRM) with Synapse.

1. Synapse was installed in three virtual machines: DICOM server, Oracle database, and storage server.
2. Storage array technology was used to replicate Logical unit Numbers (LUNs) asynchronously between a primary and secondary site.
3. Setup of protection group and recovery plans were created in VMware Site Recovery Manager.
4. A non-disruptive test of the recovery plan was run.

In this document, we refer to the "primary" and "secondary" datacenter sites. VMware also refers to these as "protected" and "recovery" sites, respectively. Storage replication here occurs one-way from the primary/protected site to the secondary/recovery site, although it is possible to configure Site Recovery Manager and SAN storage replication to protect in both directions.

Components

The following sections summarize the components deployed in this solution.

VMware Site Recovery Manager

VMware Site Recovery Manager is a disaster recovery management and automation solution for VMware® vSphere™ 4 and VMware® Infrastructure 3. Site Recovery Manager accelerates recovery by automating the recovery process and simplifying the management of disaster recovery plans. It makes disaster recovery an integrated element of managing your VMware virtual infrastructure. The solution ensures reliable recovery by eliminating complex manual recovery steps and enabling non-disruptive testing of your recovery plans. Site Recovery Manager integrates tightly with VMware Infrastructure, VMware® vCenter, and storage replication software from leading storage vendors to make failover and recovery rapid, reliable, affordable and manageable. It enables organizations to take the risk and worry out of disaster recovery, as well as expand protection to all of their important systems and applications.

Figure 1 depicts the technical architecture of Site Recovery Manager with storage array replication across two sites.

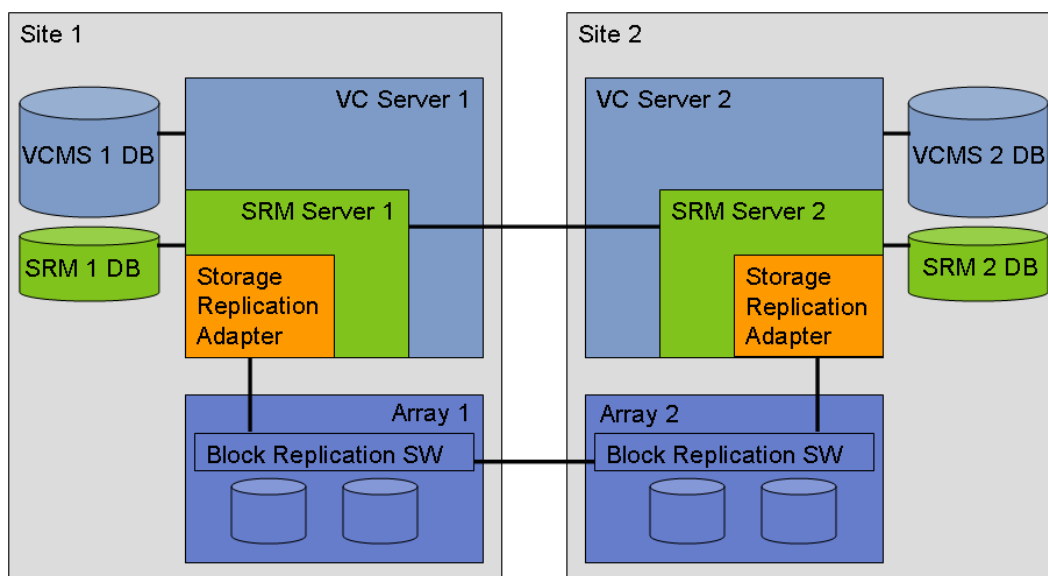


Figure 1: Site Recovery Manager Architecture

Site Recovery Manager is a plug-in to vCenter, so you can execute disaster recovery tasks from the same centralized interface that you use to manage other virtual machine administrative tasks such as creation, migration, deletion, and so forth. However, Site Recovery Manager is not a built-in component of vCenter; it is a separate server process with its own separate database. The server processes for Site Recovery Manager and vCenter can co-exist on the same server or reside on different servers. Similarly, you can create both Site Recovery Manager and vCenter data repositories in a single database or in separate databases.

Site Recovery Manager does not actually perform the replication for disaster recovery but facilitates the setup, test, and recovery workflows. Site Recovery Manager relies on block-based replication (fiber or iSCSI) from VMware storage partners for replication. Storage replication adapters that are

developed, qualified, and supported by the storage vendor manage the communication between Site Recovery Manager and the storage replication. These adapters exist on the Site Recovery Manager server and, once installed, are invisible for the duration of their use.

Third Party SAN Storage and Data Replication

VMware Site Recovery Manager Software has been tested and deployed in a variety of storage area network (SAN) environments. The following link provides access to a list of the storage replication adapters that are currently supported by VMware and its storage partners for use with SRM 10 and 1.0 Update 1: http://www.vmware.com/pdf/srm_storage_partners.pdf

Fujifilm solutions are typically deployed using EMC storage with synchronous replication. While the lab validation described here uses asynchronous replication, the recovery plan testing from within Site Recovery Manager is similar when using synchronous replication. EMC storage technology ensures database consistency when using synchronous replication with EMC MirrorView/S, which ensures write-order consistency from the source to the target.

Fujifilm Synapse® Overview

Fujifilm's Synapse™ PACS® (picture archiving and communication system) is a collection of software modules built on the Microsoft® Windows® Server platform, which together provide the core software functionality for the product. The server software communication with the workstation is entirely web based and uses Microsoft Internet Information Server (IIS) to provide image access to client workstations.

Synapse consists of the following server modules:

Database Server

The Synapse database operationally tracks all aspects of the PACS. The database supports the system folder structure, which organizes the patients and studies. All workstations communicate with the database through Hyper Text Transfer Protocol (HTTP) communication. Synapse uses Oracle 10g as its database foundation.

Web Server

Synapse uses Windows Internet Information Server (IIS) as its core Web server. Synapse is a Web-based system – all data going to and from the Synapse workstation goes through the Web server(s). All images, information and user authentication are sent over standard Web ports – port 80 for standard communication and port 443 for SSL are typical in most installations.

Storage Server

Synapse storage servers are Windows servers that are used for the storage and distribution of images, documents and other Synapse file objects. Storage directories are then presented as Universal Naming Convention (UNC) paths to the Web servers, which wrap the file content for Web-based distribution to the Synapse workstation.

DICOMServer

Synapse DICOMServer software receives studies directly from DICOM modalities without the need for modality interface gateways or interface units. All modalities are direct TCP/IP connections to the network. Synapse DICOMServer software also provides direct, brokerless DICOM Modality Worklist Management (DMWL) to any modality supporting this functionality and responds to all query/retrieve, modality performed procedure step and storage commitment requests.

HIS Server

The HIS (Hospital Information System) Synapse RIS Interface Software is integrated as an HL-7 interface engine, which provides direct brokerless connections to any HL-7 information system. It supports patient, order and report related information. Admit/Discharge/Transfer (ADT) related information could originate from the RIS or HIS.

Synapse Server

Figure 2 depicts the architecture of the Synapse servers.

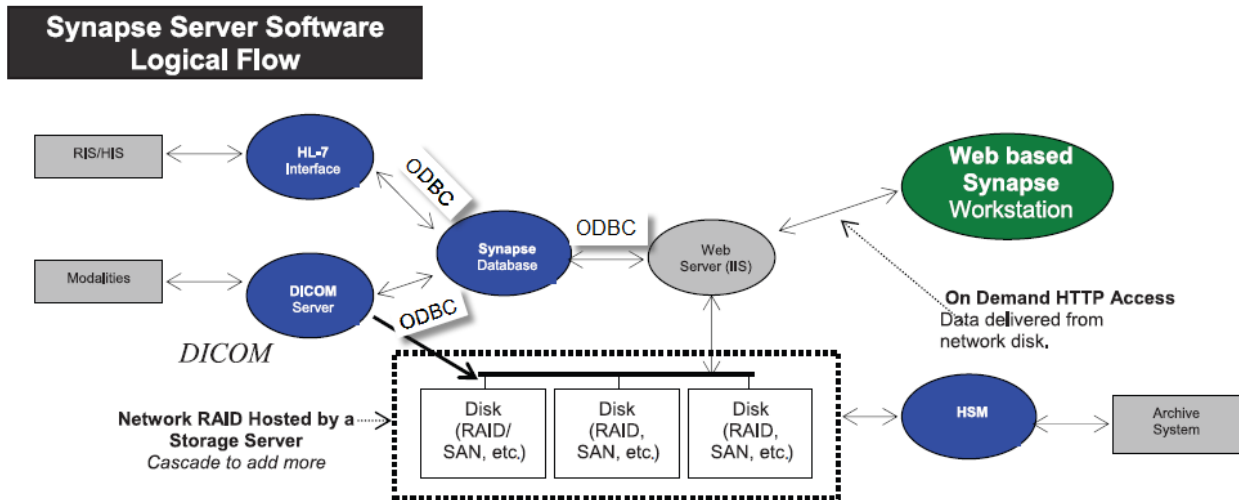


Figure 2: Synapse Server Architecture

Solution Design and Setup

Architecture

Figure 3 highlights the logical architecture for this solution. Disaster recovery testing with Site Recovery Manager requires that the virtual machines at the secondary site start from storage that is copied from the target LUNs on secondary site. This practice ensures the test is run against a storage infrastructure that is isolated from the production environment.

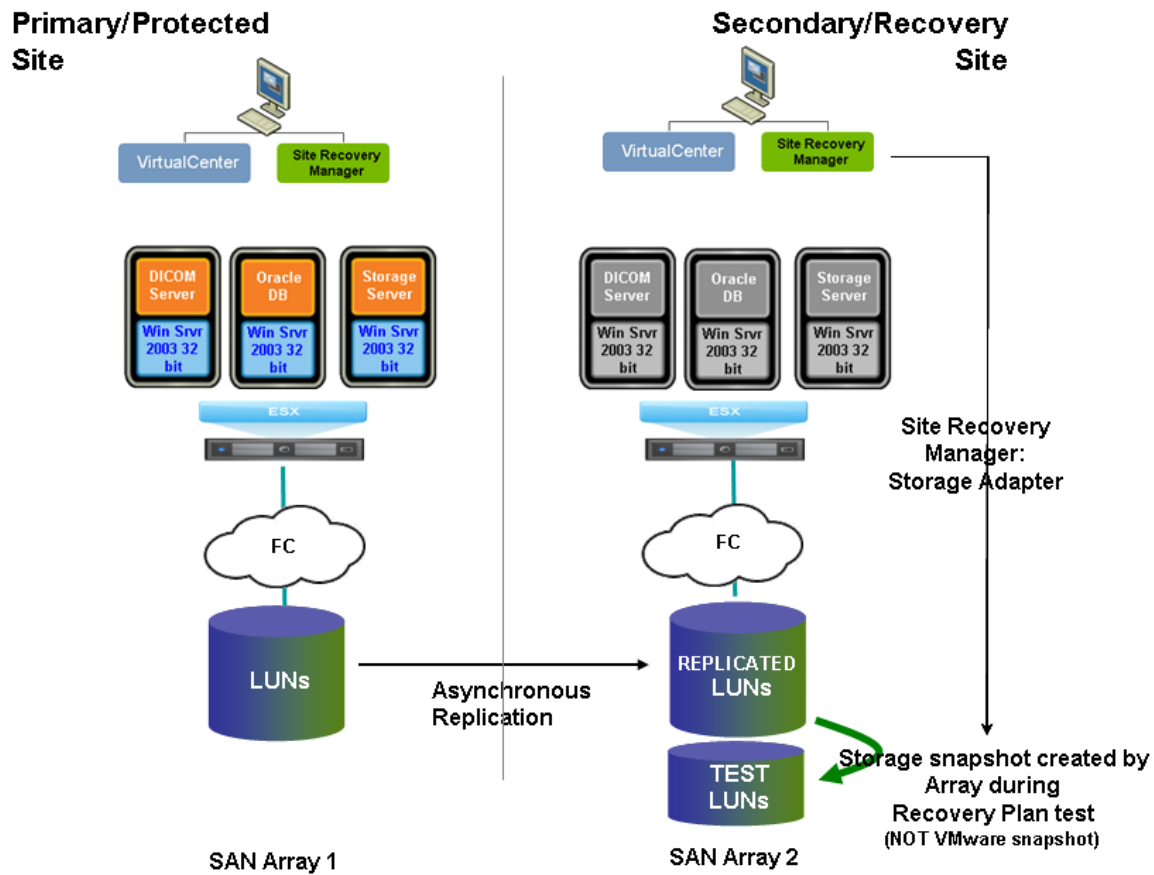


Figure 3: Site Recovery Manager Logical Architecture

Figure 4 illustrates the physical architecture for this solution.

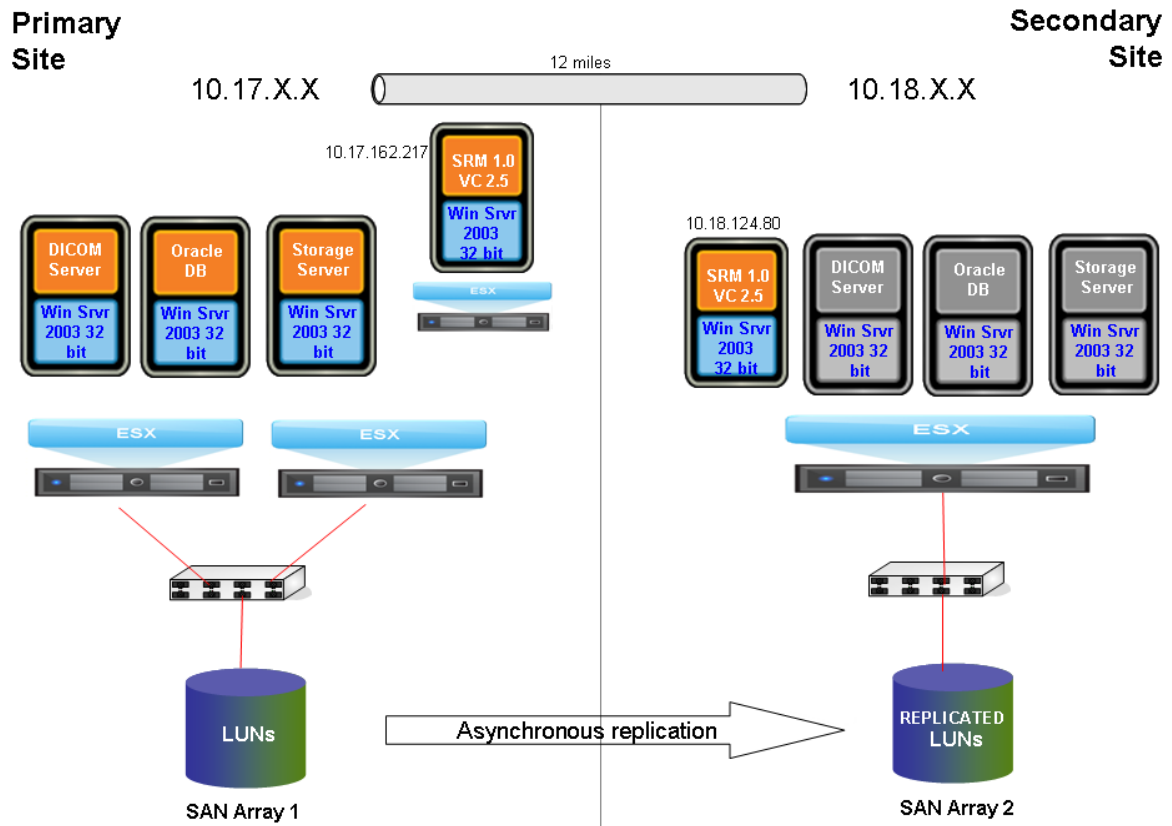


Figure 4: Site Recovery Manager Physical Architecture

Software Used

The following table lists the software used in the architecture.

VMware	
VMware Infrastructure 3	vCenter Server 2.5 VMware® ESX 3.5
Site Recovery Manager	Site Recovery Manager 1.0 Update 1
FUJIFILM	
Synapse Server	<u>Virtual Machine "tapstor1"</u> Storage server 1 x vCPU 512MB RAM Windows Server 2003 R2 EE SP2 32-bit "C" drive is VMFS storage (10 GB) 1 x drive is RDM (50 GB LUN) - stores images, generally a 2TB LUN in production <u>Virtual Machine "tapdb1"</u> Oracle database 2 x vCPU 512MB RAM Windows Server 2003 R2 EE SP2 32-bit All drives VMFS storage (66GB total) <u>Virtual Machine "tapdicom1"</u> DICOM print server 2 x vCPU 512MB RAM Windows Server 2003 R2 EE SP2 32-bit All drives VMFS storage (30GB total)

Figure 5 shows the three virtual machines in vCenter.

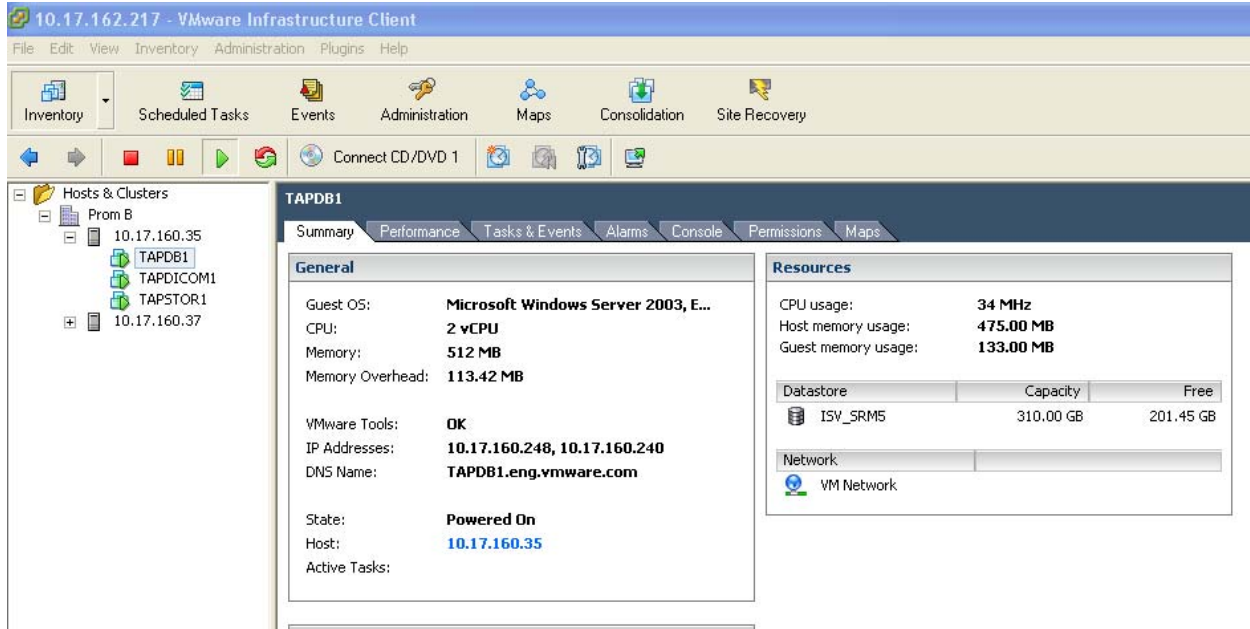


Figure 5: Synapse Virtual Machines in vCenter (Primary Site)

Key points about this setup:

- Site Recovery Manager requires two vCenter Server instances - one each at the primary and secondary sites. For this validation (built in two labs separated by 12 miles), the vCenter instances were running in virtual machines. On the primary site we used a dedicated ESX host to run the primary vCenter instance. At the secondary site the vCenter virtual machine ran on a single ESX host that was also used for recovered virtual machines.

Note: The best practice would normally place the secondary vCenter instance on a dedicated server separated from the servers that are hosting recovered virtual machines.

- For data replication, asynchronous mode was configured to replicate all the related LUNs from the primary to the secondary site.
- The Storage Replication Adapter (SRA) was installed on the primary and secondary vCenter servers. The value of the SRA is that it:
 - Automatically discovers the replicated LUNs on the primary site.
 - Facilitates a Site Recovery Manager test workflow on the secondary site and creates a clone of the replicated LUNs.
- All virtual machines were configured as Virtual Machine File System (VMFS) storage except for the storage server "tapstor1" which included a Raw Device Mapping (RDM) disk that stored the medical images.

The screen capture in figure 6 below shows the RDM configuration.

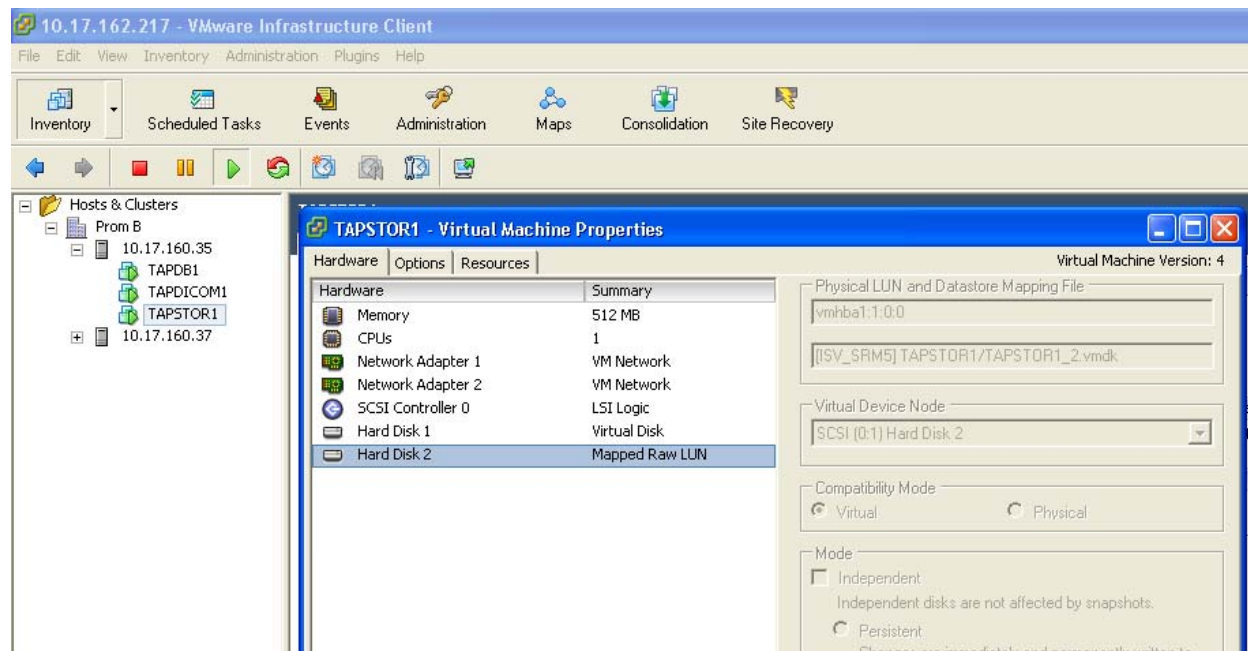


Figure 6: Storage Settings of Storage Server Virtual Machine - Includes one RDM disk (Primary Site)

Hardware and Software Configuration

The hardware and software were installed and configured using this step-by-step process:

- Configure storage arrays at the primary and secondary sites.
- Create LUNs on the primary site storage and expose to primary site ESX host server.
- Install vCenter Server 2.5 on two Windows virtual machines. These virtual machines will serve as the primary and secondary site vCenter Server instances.
- Install Synapse virtual machines on primary site.
- Configure storage replication between the primary and secondary site storage arrays.
- Install and configure Site Recovery Manager on the primary and secondary vCenter Server instances (see next section).

Site Recovery Manager Installation and Configuration

The following sections provide a high-level overview of Site Recovery Manager installation and configuration. For detailed configuration steps, please consult Appendix A and the VMware product guides referenced in Appendix B.

Primary and Secondary site:

- Install the Site Recovery Manager server into a separate database instance on the same guest OS that is running vCenter Server. (Please note: This procedure was followed for this installation, but other install options are available that allow the SRM server to reside on an OS image/server that is separate from vCenter).

- Install Site Recovery Manager Plug-in into vCenter.
- Install Storage Replication Adapter (SRA) on the guest-OS of the vCenter virtual machines.

After installation, the Site Recovery Manager plug-in is available and can be accessed via the VMware® Infrastructure (VI) Client. The screenshot in Figure 7 is of the primary vCenter Server and defines the configuration steps required after the initial installation; you will need to execute the steps defined here.

The screenshot shows the VMware Infrastructure Client interface. The top menu bar includes File, Edit, View, Inventory, Administration, Plugins, and Help. The main toolbar contains icons for Inventory, Scheduled Tasks, Events, Administration, Maps, Consolidation, and Site Recovery. The left sidebar shows a tree view with Site Recovery, Protection Groups, and Recovery Plans. The main content area displays the configuration for a primary site named 'Prom B'.

Local Site		Paired Site	
VC Server:	10.17.162.217:443	VC Server:	10.18.124.80:443
SRM Server:	10.17.162.217:8095	SRM Server:	10.18.124.80:8095
Site Name:	Prom B	Site Name:	OSDC

Protection Setup	
Use the steps below to configure protection for this site.	
Connection:	Connected Configure Break
Array Managers:	Configured Configure
Inventory Mappings:	Configured Configure
Protection Groups:	4 Create

Recovery Setup	
Create recovery plans for protection groups on the paired site.	
Recovery Plans:	No Plans Created Create

Figure 7: SRM Screen shot of Summary Tab (Primary Site)

Primary Site:

- Configure the connection between primary and secondary Site Recovery Manager servers.
- Configure the array manager.
- Configure your inventory preferences.
- Create the protection group "FUJI" for the virtual machines at the primary site.

Secondary Site:

- Create recovery plan "FUJI" consisting of group "FUJI."

- When you create a recovery plan, you have the option to suspend non-critical virtual machines that are running at the secondary site. (In most cases, the hardware on the secondary site can be and is used to host virtual machines so it is not idle during normal operations).
- Prioritize virtual machines start-order as required.
- You have the option to:
 - Create a custom specification for the virtual machines so that they start up on the secondary site on a different subnet from the primary site, or
 - Perform no custom specification and configure the virtual machines to start up in a private test network bubble with the same networking parameters as the primary site.

Disaster Recovery Testing

Disaster recovery testing comprises a logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time following a disaster or an extended disruption. This logistical plan is commonly referred to as the Business Continuity (BC) Plan. Common wisdom states that any disaster recovery plan is only as good as your last (successful) test. Indeed, most disaster recovery efforts fail because of one of two factors: the team either spends an inordinate amount of effort conducting continuous tests or -- worse -- neglects to test often. Either way, the result is an insurance policy that does not pay off when disaster hits.

Disaster recovery testing is often difficult because it is usually very disruptive, expensive in terms of resources, and extremely complex. However, by leveraging virtualization, VMware Site Recovery Manager addresses these problems while making planning and testing simpler to execute. Site Recovery Manager has the ability to recover virtual machines and network connections that can be tested as a walled-off virtual entity - perhaps even co-resident with production applications that might be running at the remote site. This ability to encapsulate and test a complete recovery scenario in a set of virtual machines greatly simplifies the task and saves significant time and resources.

You can also run frequent tests that simulate an actual recovery by running a recovery plan test. Site Recovery Manager runs exactly the same plan for both tests and actual recoveries with the following exceptions:

- Recovery tests do not connect to the primary site and shut down virtual machines.
- From a network perspective, recovery tests have two options:
 - Create a test bubble network that is removed after the test is completed. If there is only one ESX host server, the automatically generated test bubble network connects the virtual machines together via a private virtual switch and traffic does not leave that switch to prevent interference with the secondary site network. When there are multiple hosts on the secondary site, the private virtual switch method does not work as it does not span hosts. The solution to this limitation is to use an isolated VLAN, documented at this URL: <http://blogs.vmware.com/uptime/2009/01/how-to-exploit-the-test-bubble-for-all-its-worth.html>
 - Alternatively, create a custom specification for the virtual machines so that they start up on the secondary site on a different subnet from the primary site. Although we are discussing options for a recovery test, network customization settings would be used for an actual recovery and more details can be found in the following paper, *Automating Network Setting Changes and DNS Updates on Recovery Site Using VMware vCenter Site Recovery Manager* available here: <http://viops.vmware.com/home/docs/DOC-1449>

The recovery test documented here uses the test network bubble scenario and the configuration steps for that are shown in Appendix A.

Execute Recovery Plan Test

The following sequence was executed to validate the recovery plan test:

- Start Site Recovery Manager disaster recovery test on secondary site for recovery plan "FUJI".

- Once the Recovery Plan test completes, press "Continue" to ensure proper cleanup.

During the recovery test, SRM starts the virtual machines defined in the recovery plan and then stops and waits for user input before performing a cleanup and removal of the recovered virtual machines and storage. The screen capture in Figure 8 shows this operation.

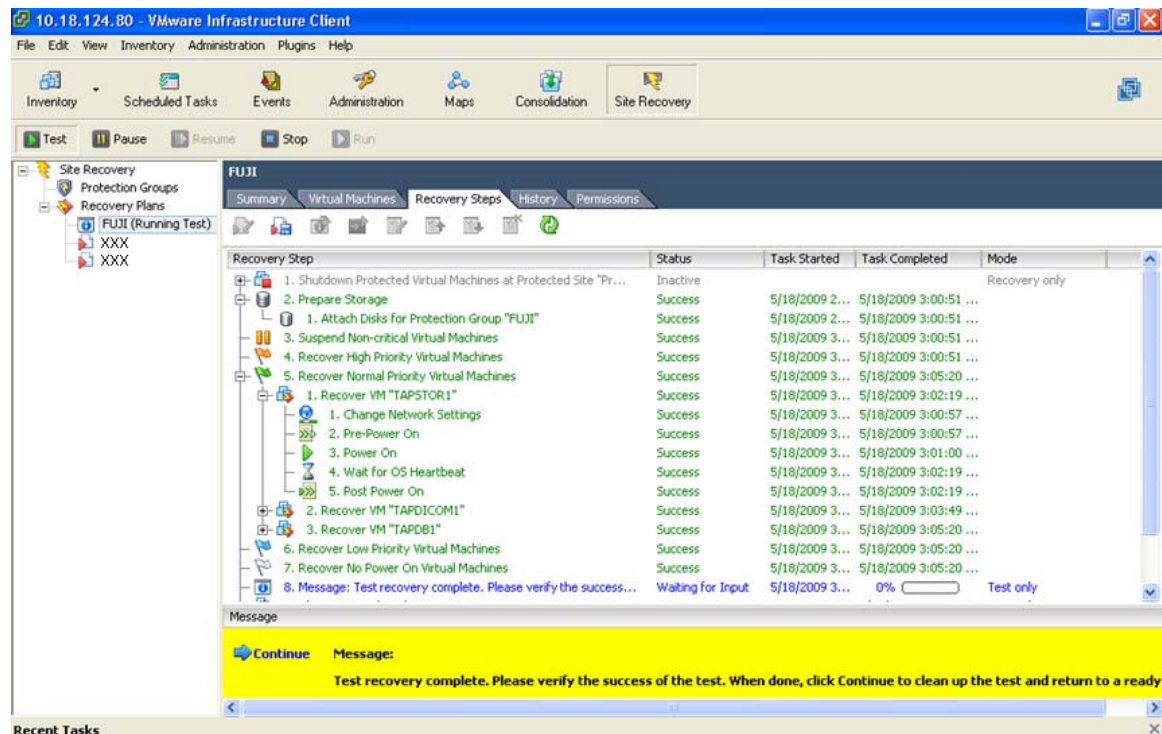


Figure 8: Recovery Plan Steps during Test Recovery of FUJI Virtual Machines (Secondary Site)

Meanwhile, the virtual machines are up and running in vCenter and can be accessed for user testing. In this example, the virtual machines are started in a test bubble network with the same network parameters as in the primary site. Figure 9 shows the creation of a virtual network "testBubble-1," which SRM creates automatically during the recovery test workflow.

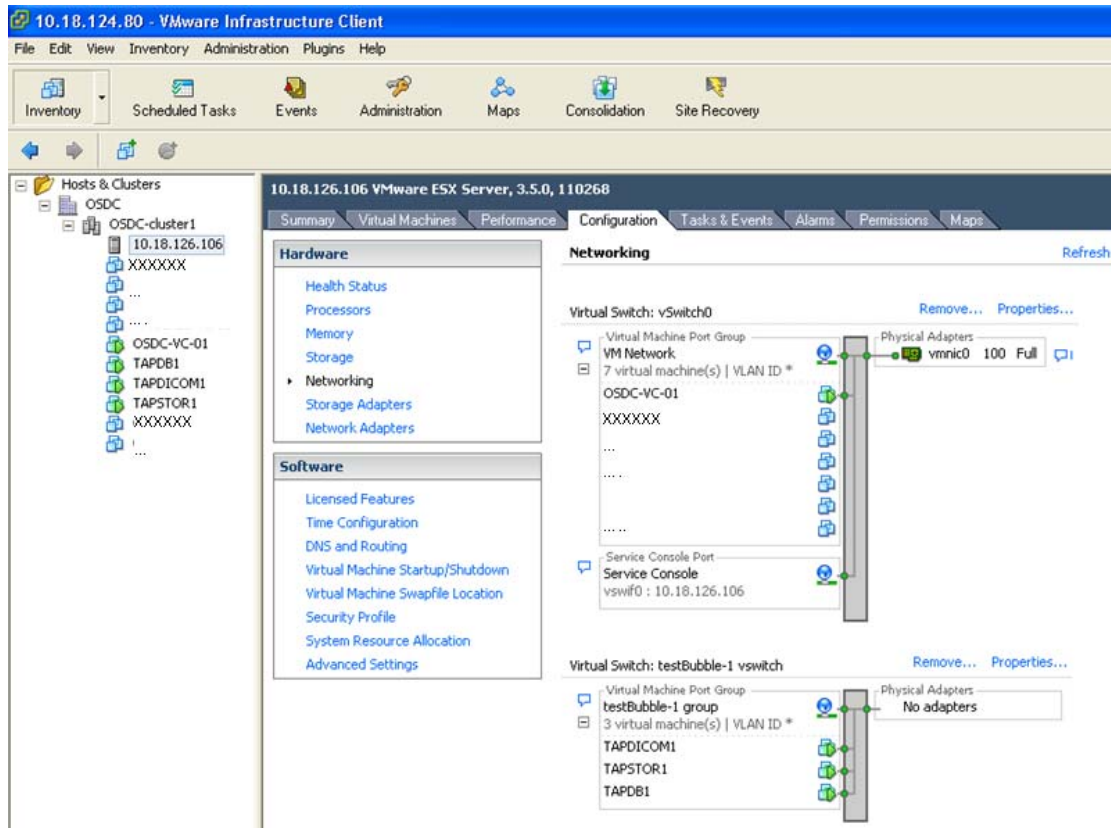


Figure 9: Test Bubble Network (Secondary Site)

Synapse can also be tested within this network bubble and the three virtual machines can communicate with each other, but not with any entity outside of this bubble. The RDM drive for virtual machine "tapstor1" is also appropriately recovered and correctly associated with its parent virtual machine as shown in Figure 10.

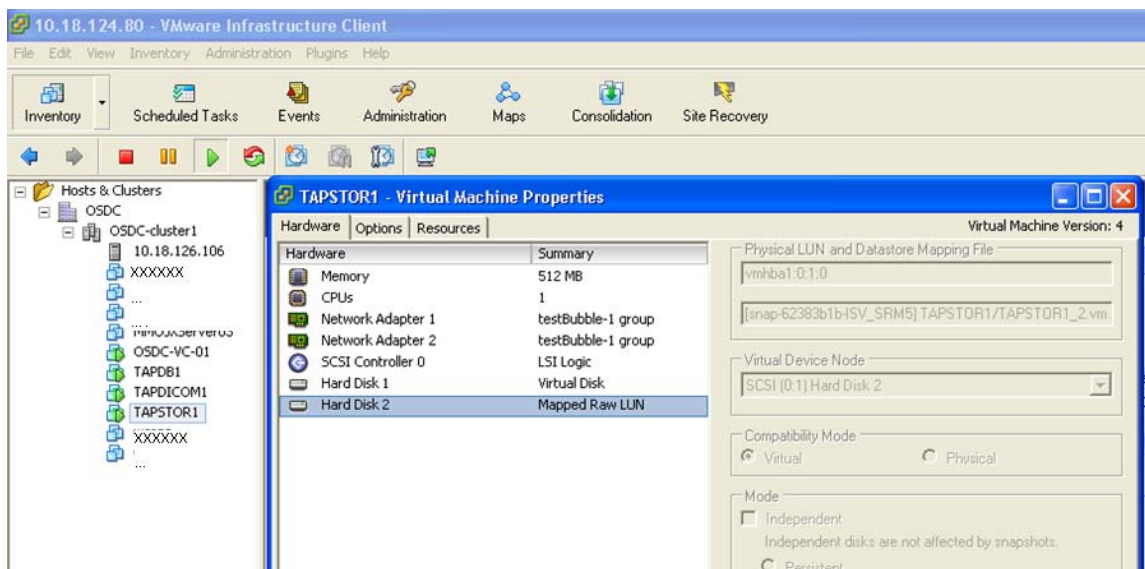


Figure 10: Storage Settings of RDM disk of Recovered Virtual Machine "tapstor1" (Secondary Site)

Testing showed that every component (Oracle database, DICOM Server, Codebase server) came up and functioned as expected. DiskXtender was also tested by purging and retrieving a managed file and this operation was successful.

Once the testing was complete, the history of the recovery plan test was saved in SRM, thus capturing all the details of each recovery step; this history can be used for auditing purposes. Figure 11 shows the beginning of the report (the complete output is not shown).

Recovery Step	Result	Execution Time
1. Shutdown Protected Virtual Machines at Protected Site "Prom B"		
1.1. Shutdown Low Priority Protected Virtual Machines		
1.2. Shutdown Normal Priority Protected Virtual Machines		
1.2.1. Shutdown Protected Site VM "TAPSTOR1"		
1.2.1.1. Shutdown Guest OS for Remote VM "TAPSTOR1"		
1.2.1.2. Wait for Guest OS Shutdown		
1.2.1.3. Power off VM "TAPSTOR1"		
1.2.2. Shutdown Protected Site VM "TAPDICOM1"		
1.2.2.1. Shutdown Guest OS for Remote VM "TAPDICOM1"		
1.2.2.2. Wait for Guest OS Shutdown		
1.2.2.3. Power off VM "TAPDICOM1"		
1.2.3. Shutdown Protected Site VM "TAPDB1"		
1.2.3.1. Shutdown Guest OS for Remote VM "TAPDB1"		
1.2.3.2. Wait for Guest OS Shutdown		
1.2.3.3. Power off VM "TAPDB1"		
1.3. Shutdown High Priority Protected Virtual Machines		
2. Prepare Storage	Success	00:01:05
2.1. Attach Disks for Protection Group "FUJI"	Success	00:01:05
3. Suspend Non-critical Virtual Machines	Success	00:00:00
4. Recover High Priority Virtual Machines	Success	00:00:00
5. Recover Normal Priority Virtual Machines	Success	00:04:28
5.1. Recover VM "TAPSTOR1"	Success	00:01:27
5.1.1. Change Network Settings	Success	00:00:06

Figure 11: History of Recovery Plan Test (Secondary Site)

Execute Recovery Plan Actual

Running an actual recovery plan starts the virtual machines on the secondary site network. This process cannot be undone automatically and it permanently alters the infrastructure of the primary and secondary sites. The following changes occur if you run a recovery plan:

- During a recovery, if the primary site is connected to the secondary site, virtual machines shut down gracefully on the protected site.
- If the connection between sites is lost, SRM takes no action against the protected virtual machines in the primary site. The datastores in the recovery site are enabled for read and write capabilities and SRM initiates the power up of the virtual machines in the recovery site according to the startup order in the recovery plan.
- The virtual machines are started on the secondary/recovery site network and are assigned network parameters based on guest customization.

Managing failback using VMware Site Recovery Manager is a manual process that is covered in more detail in the *VMware Site Recovery Manager Administration Guide* located here:

http://www.vmware.com/pdf/srm_10_admin.pdf

Conclusion

This document demonstrates how VMware Site Recovery Manager enables the design of an effective and automated disaster recovery solution. Within a multi-tier Fujifilm Synapse environment, Site Recovery Manager enables you to:

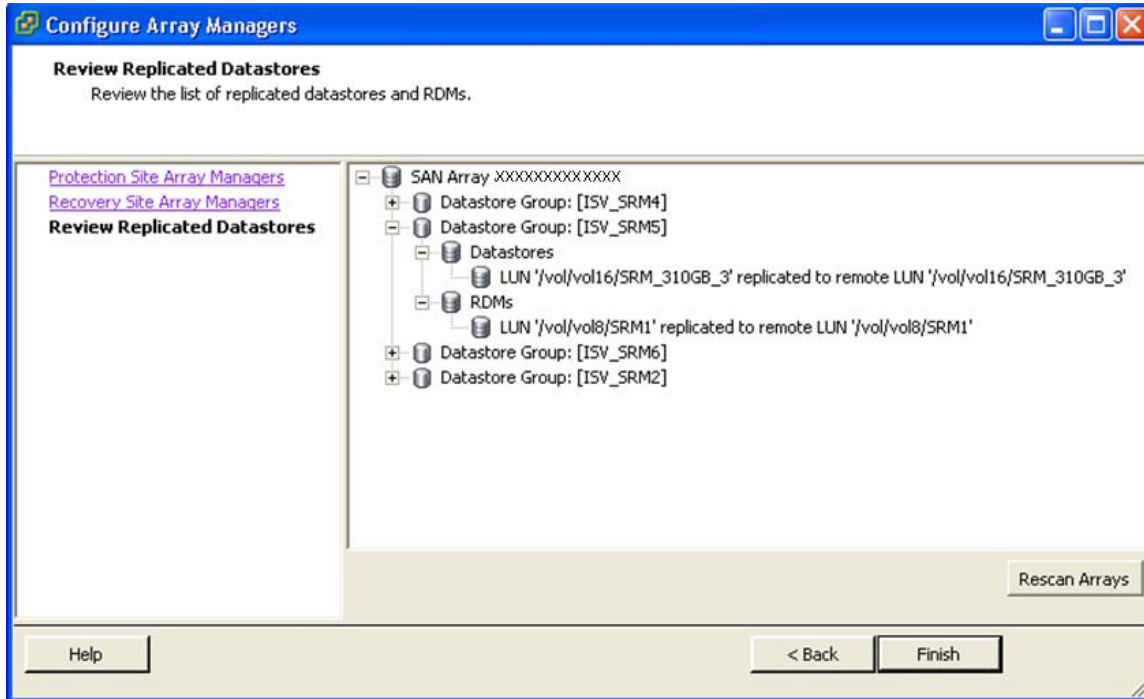
- Accelerate recovery of the virtual environment through automation. The recovery of Fujifilm virtual machines into a different subnet or test bubble network on the secondary site is fully automated.
- Ensure reliable recovery by enabling non-disruptive testing. Recovery plan testing can be conducted as many times as required to satisfy auditing requirements.
- Simplify recovery by eliminating complex manual recovery steps and centralizing management of recovery plans.

Traditional disaster recovery solutions are slow and prone to failures because they involve many manual and complex steps that are difficult to test, and they require expensive duplication of the production datacenter infrastructure to ensure reliable recovery. VMware Site Recovery Manager is designed to simplify and automate the disaster recovery process so that you can reliably recover from datacenter outages in hours rather than days. Along with VMware Infrastructure or VMware vSphere, VMware Site Recovery Manager can help eliminate the complexity and unreliability of manual recovery and do away with the cost and complexity of maintaining duplicate but idle infrastructure at a recovery site.

Appendix A: Site Recovery Manager Setup

Configure Storage Array Manager (Primary Site)

Storage array manager is configured on the primary site vCenter under Site Recovery manager -> click on "Array managers." The complete steps are not shown here. During the configuration SRM automatically detects the datastores that are being replicated and displays them in the configuration wizard. See the following screen capture.



The figure shows that the RDM for the storage server virtual machine "tapstor1" is automatically detected by SRM.

Configure Inventory mappings (Primary Site)

As shown in the following screen capture, it is recommended to configure inventory preferences to provide mappings between compute resources, virtual machine folders, and networks on the primary site and their counterparts on the secondary site.

The screenshot shows the VMware Infrastructure Client interface for Site Recovery Manager. The 'Inventory Mappings' tab is active, displaying a table with the following data:

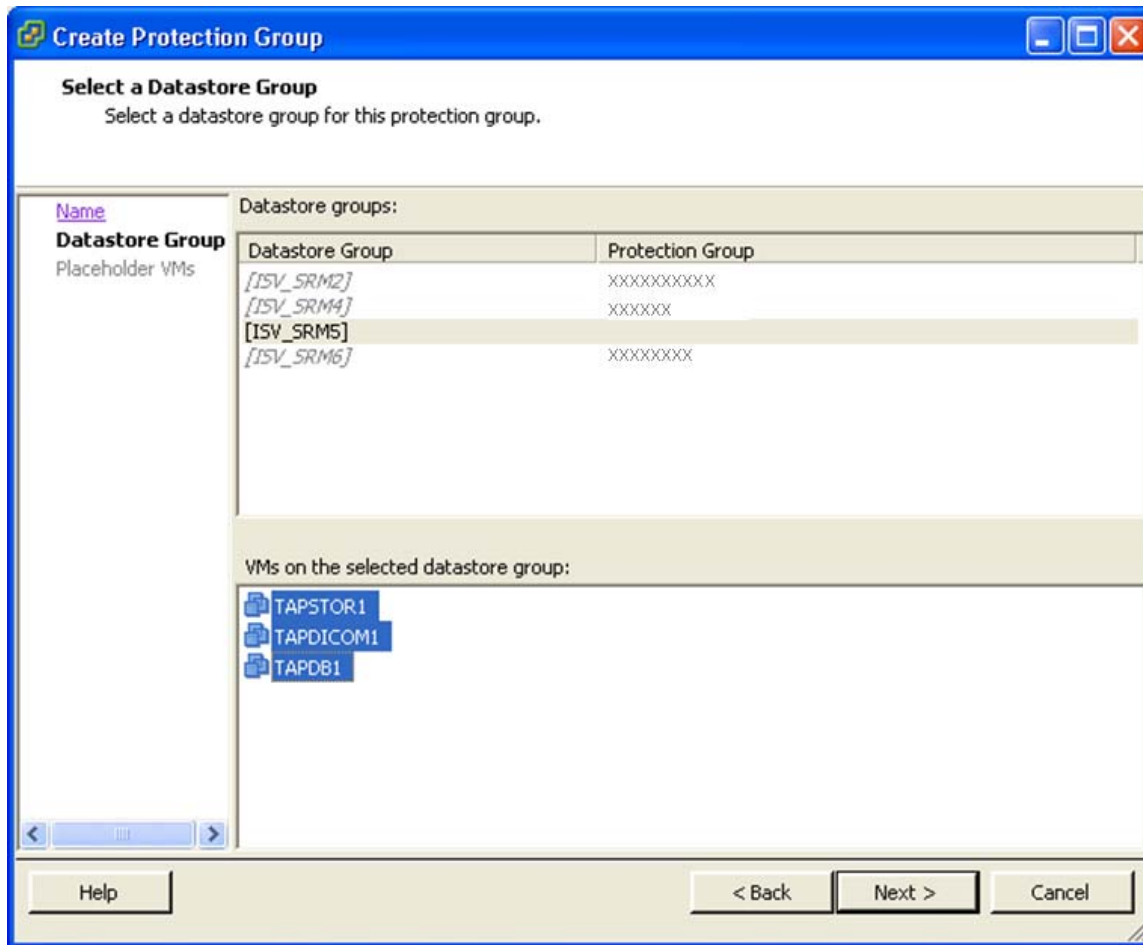
Protection Site Resources	Recovery Site Resources	Recovery Site Path
Networks		
Prom B	---	
VM Network	VM Network	/Networks/
Compute Resources		
Prom B	---	
10.17.160.35	OSDC-cluster1	/Hosts & Clusters/OSDC/
10.17.160.37	OSDC-cluster1	/Hosts & Clusters/OSDC/
Virtual Machine Folders		
Prom B	OSDC	/Datacenters/
Discovered Virtual Machine	OSDC	/Datacenters/

Create Protection Group (Primary Site)

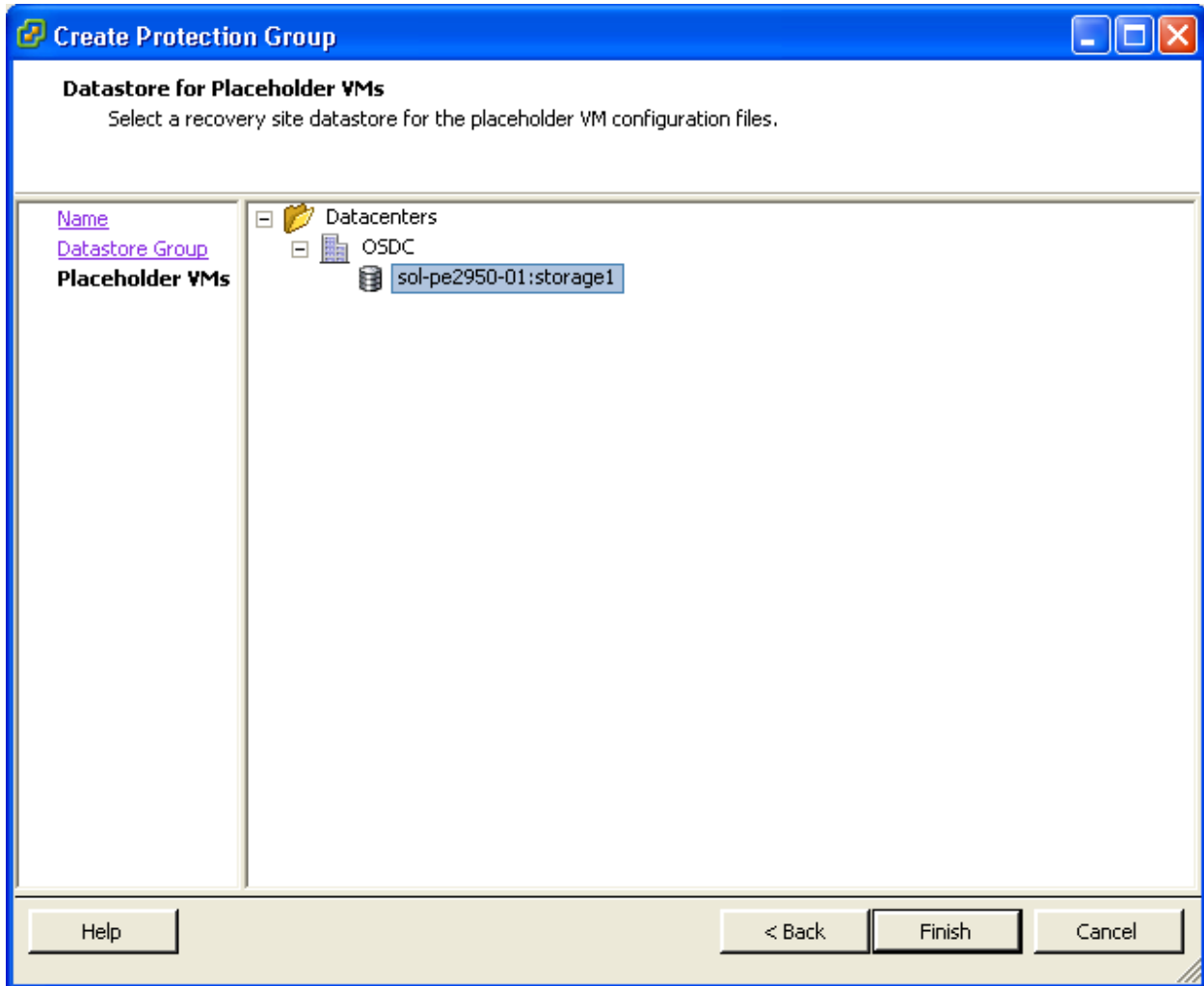
A protection group is a group of virtual machines that fail over together at the recovery site during test and recovery. When you set up a protection group, placeholder virtual machines are created on the recovery site. These placeholder virtual machines, sometimes referred to as recovery virtual machines, are visible in the recovery site inventory. The placeholder machine represents a protected virtual machine in the protected site and does the following:

- Provides a cue that the original machine in the protected site is protected.
- Indicates where the protected machine is recovered in the recovery inventory.

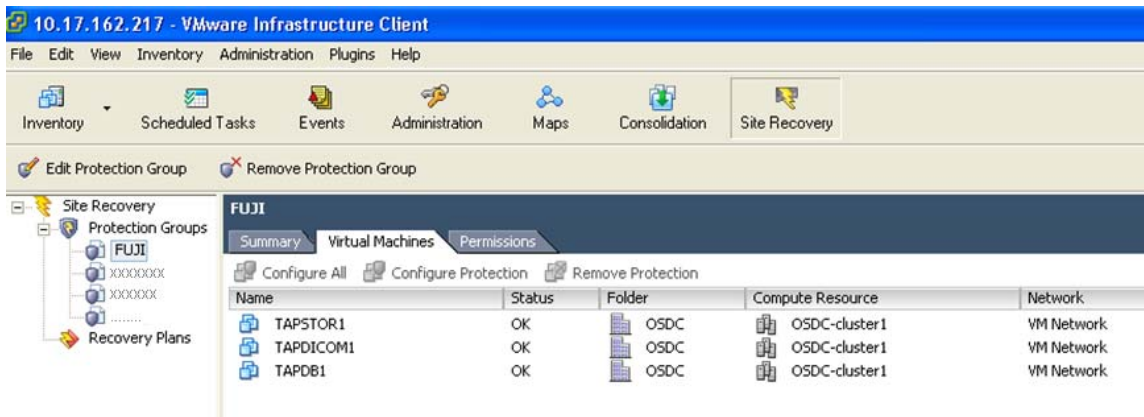
The following screen captures show parts of the Create Protection Group process in Site Recovery Manager. The datastore with the Fujifilm virtual machines is assigned to the protection group.



On the secondary site, assign a LUN location to the placeholder configuration files of the protected virtual machines as shown in the next screen capture.

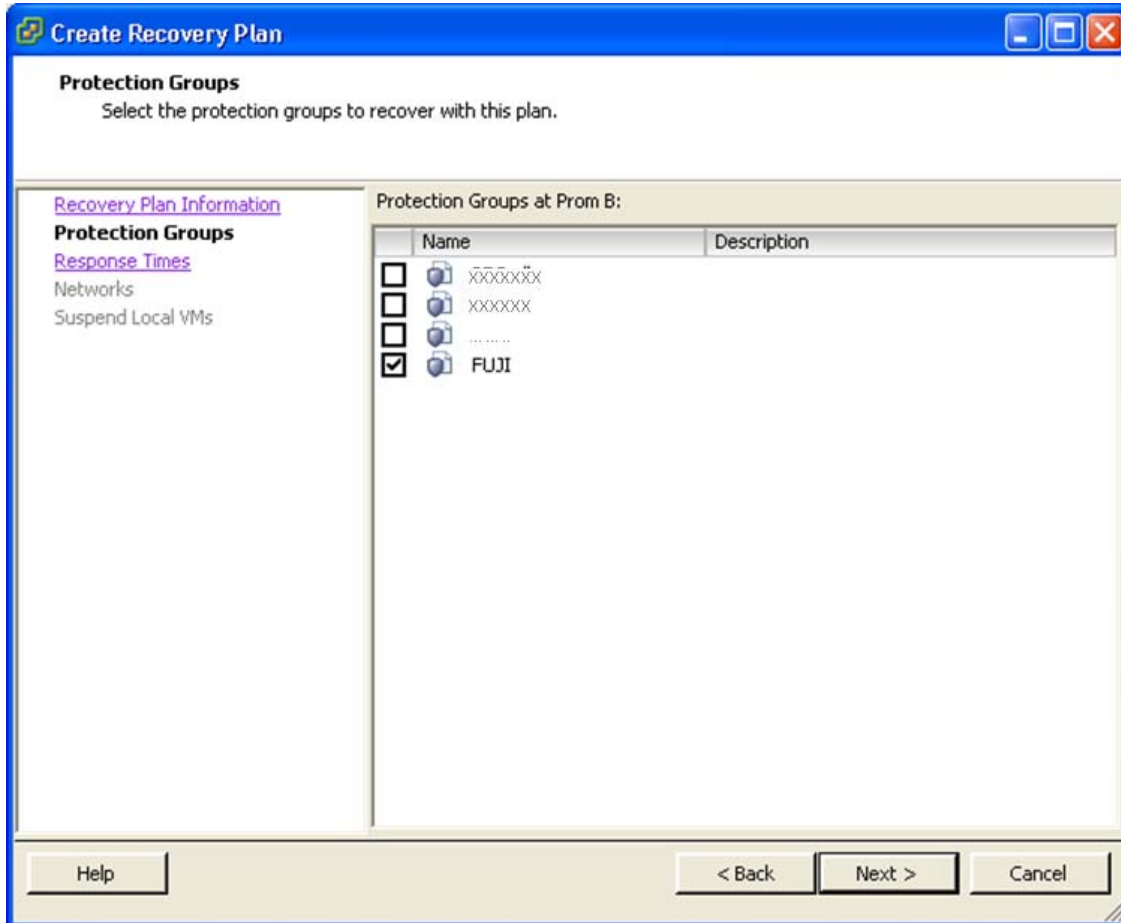


The resulting protection group is shown here.

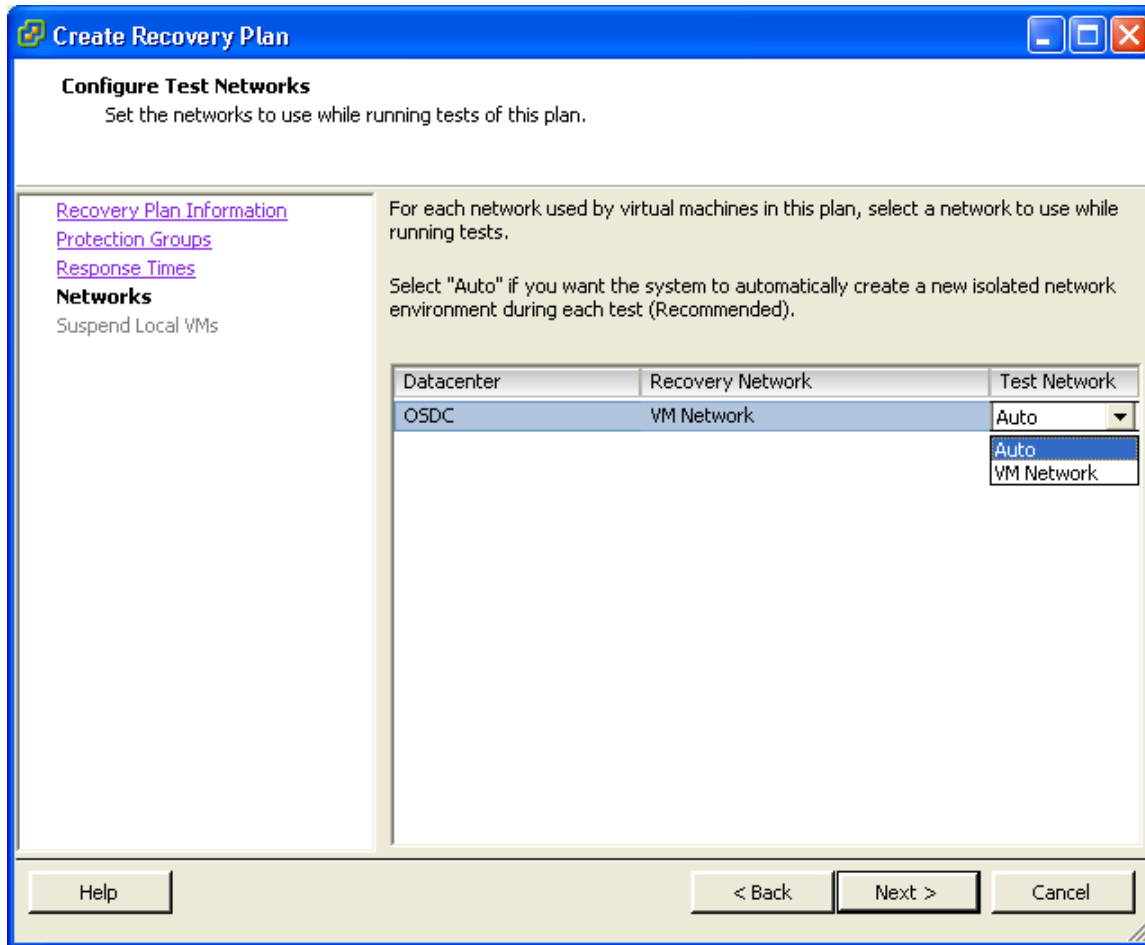


Create Recovery Plan (Secondary Site)

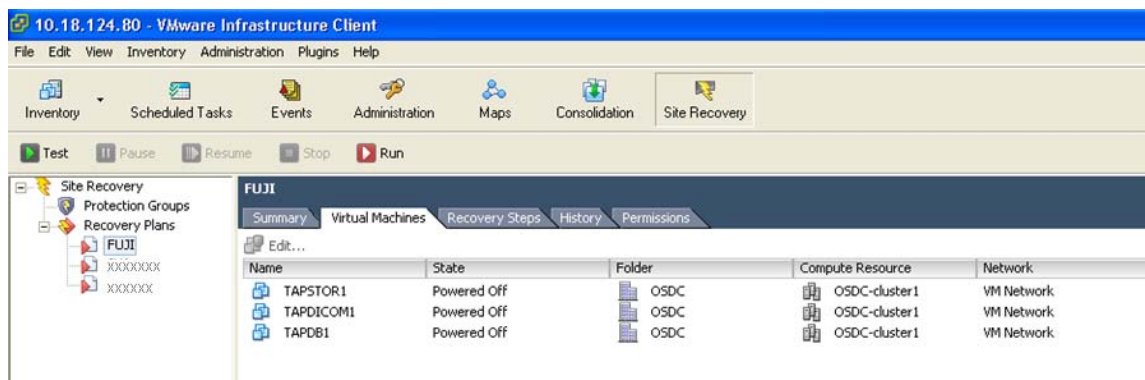
The Recovery Plan Wizard prompts you to create a plan name and assign the protection group to the plan. The virtual machines are automatically assigned to the plan based on the protection group. Some of the create recovery plan wizard steps are shown here. The next screen capture shows how the "Fujifilm" protection group is assigned to the plan. All the virtual machines defined in the "Fujifilm" protection group are now automatically included in the recovery plan.



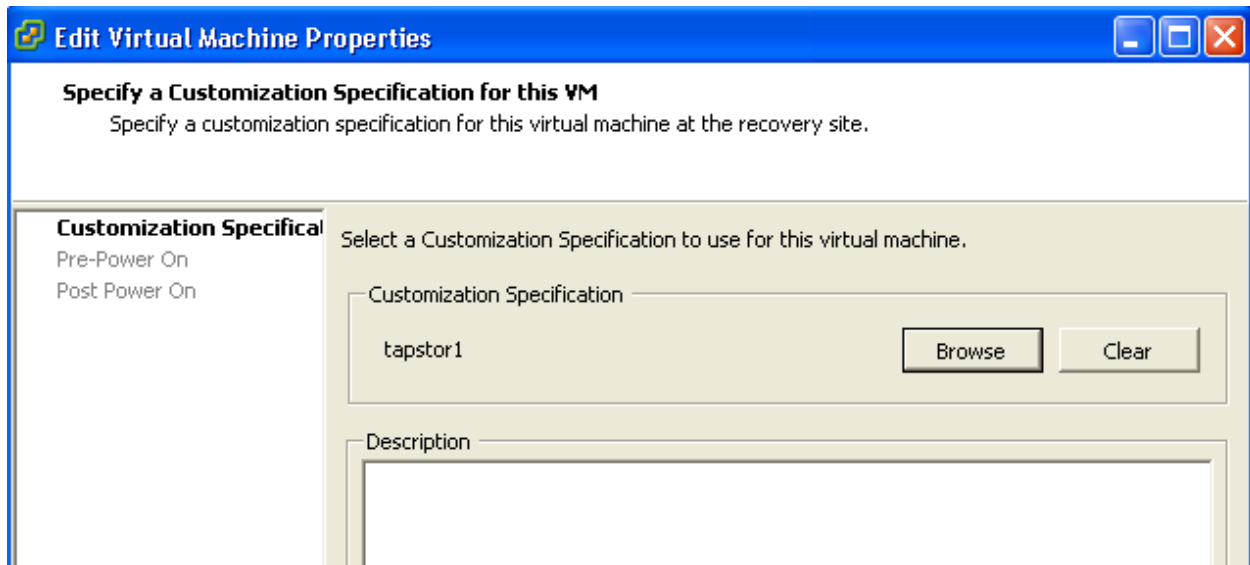
The next screen capture shows where the recovery network is specified. In this example we chose "Auto," which means the virtual machines are recovered into a test bubble network. "VM Network" refers to the main network on the secondary site.



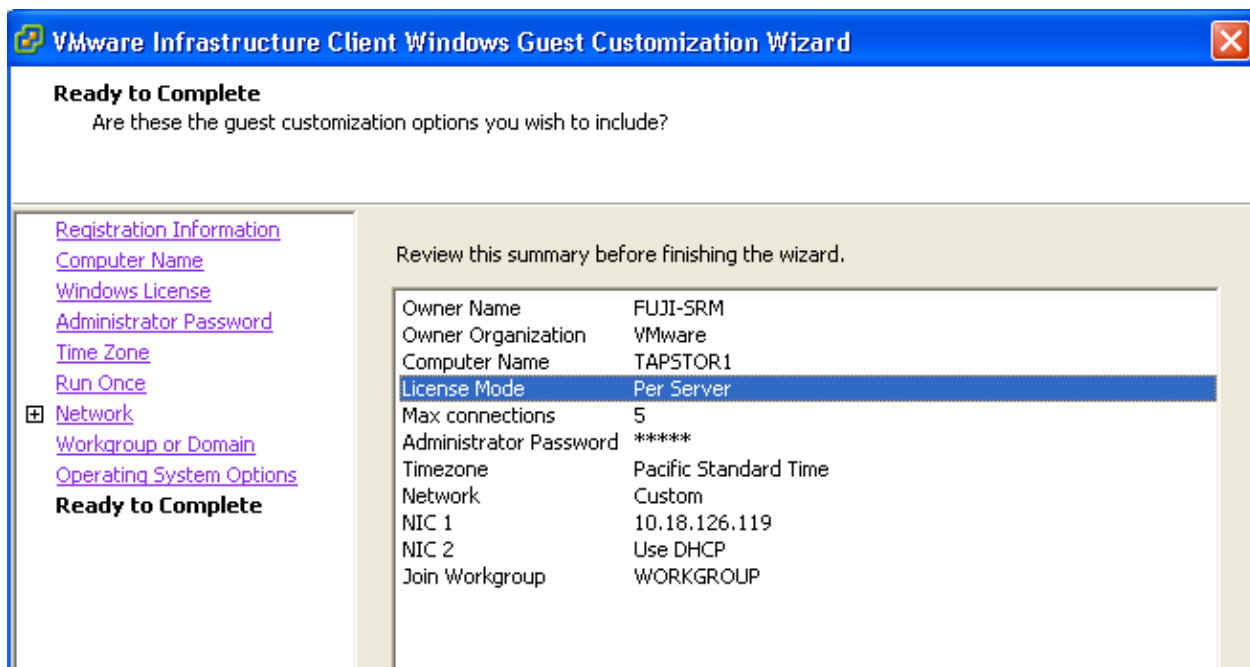
The resulting recovery plan is shown here.



From the previous screen, it is possible to assign a guest customization to each virtual machine by selecting the virtual machine and clicking on "Edit" to bring up the following screen on which you can assign a pre-defined custom specification.



The custom specification has to be created first before assignment to the virtual machine as shown above. This can be done by invoking the Customization Specification Manager on the secondary site Site Recovery Manager Server (from the VI Client, select Edit > Customization Specifications). This brings up the Guest Customization Wizard in which the secondary/recovery site network parameters can be defined as shown in the screenshot below.



Configuring guest customizations for multiple virtual machines can be automated as described in the paper *Automating Network Setting Changes and DNS Updates on Recovery Site Using VMware vCenter Site Recovery Manager* available at <http://viops.vmware.com/home/docs/DOC-1449>. This paper explains:

- How a batch IP property customization tool allows you to specify network settings for any or all of the virtual machines in a recovery plan by editing a comma-separated-value (CSV) file that the tool generates. This file can then be loaded into Site Recovery Manager.
- How to manage updates of DNS server records on the secondary site.

Appendix B: References

VMware:

- VMware virtualization products page
http://www.vmware.com/products/data_center.html
- VMware Site Recovery Manager
http://www.vmware.com/files/pdf/srm_datasheet.pdf
- VMware Site Recovery Manager administration guide
http://www.vmware.com/pdf/srm_10_admin.pdf
- VMware Site Recovery Manager 1.0 Release Notes
http://www.vmware.com/support/srm/srm_10_releasenotes.html
- How to Exploit Test Bubble during SRM Recovery Test
<http://blogs.vmware.com/uptime/2009/01/how-to-exploit-the-test-bubble-for-all-its-worth.html>
- VMware Site Recovery Manager Storage Partners
http://www.vmware.com/pdf/srm_storage_partners.pdf
- Automating Network Setting Changes and DNS Updates on Recovery Site Using VMware vCenter Site Recovery Manager
<http://viops.vmware.com/home/docs/DOC-1449>

FUJIFILM:

- FUJIFILM Medical Systems USA
<http://www.fujimed.com/>



**VMware, Inc. 3401 Hillview Ave. Palo Alto CA 94304 USA Tel 1-877-486-9273
Fax 650-427-5001 www.vmware.com**

© 2008 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,961,941, 6,961,806, 6,944,699, 7,069,413; 7,082,598 and 7,089,377; patents pending.

