Disaster Recovery for
GE Centricity RIS-IC Solutions
with VMware Site Recovery Manager

August 2010

WHITE PAPER

Contributors:
GE Healthcare: Jeff Lovett, Jim Rainville, Hans Buehler
VMware: Raymond Milot, Praveen Javehrani, Pramod Mahadevan
Table of Contents

Introduction................................................................................................................................. 1
GE Centricity RIS-IC Site Recovery Overview........................................................................ 1
VMware Site Recovery Manager .......................................................................................... 3
    Third Party SAN Storage and Data Replication ............................................................. 4
    Site Recovery Use Cases ............................................................................................... 4
Solution Design and Setup..................................................................................................... 4
    Solution Architecture .................................................................................................... 4
    Physical Hardware ......................................................................................................... 6
    Installed Software .......................................................................................................... 6
    Virtual Machine Configurations .................................................................................... 7
Solution Configuration Steps ............................................................................................... 8
VMware SRM Installation and Configuration ........................................................................ 9
    Primary and Secondary site ......................................................................................... 9
    Primary Site .................................................................................................................. 9
    Secondary Site ............................................................................................................. 10
Disaster Recovery Testing .................................................................................................... 10
    Execute Recovery Plan Test ....................................................................................... 11
    Recovery Plan Execution During Actual Failover ....................................................... 12
General Recommendations ................................................................................................. 13
Summary .............................................................................................................................. 14
Additional Resources ................................................................................................ .......... 14
Appendix A: Site Recovery Manager Setup ......................................................................... 15
    Configure Storage Array Manager (Primary Site) ....................................................... 15
    Configure Inventory Mappings (Primary Site) .............................................................. 15
    Create Protection Group (Primary Site) ....................................................................... 16
    Create Recovery Plan (Secondary Site) ....................................................................... 18
Introduction

This document describes a site recovery solution for a virtualized multi-tier RIS application from GE Healthcare configured with VMware® Site Recovery Manager (SRM). From this example, you can see how VMware SRM can help you:

- 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.

Companies that have deployed the GE Centricity® RIS-IC product depend heavily on the information, processes and availability of their deployed application environments, even in the case of a disaster. However, the complexity and distributed nature of these applications 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 and block-based SAN storage replication to provide an effective availability solution for mission-critical GE Centricity RIS-IC deployments.

GE Centricity RIS-IC Site Recovery Overview

GE Centricity RIS-IC is a web-based radiology information solution designed to address evolving clinical and business needs by taking an enterprise-wide, patient-centric view of workflow that dissolves departmental boundaries and ends the paper chase. Delivering fast, secure access to information, Centricity RIS-IC helps to streamline the clinical and administrative workflow in today’s hectic Radiology departments through the application of state-of-the-art technology. Centricity RIS-IC can help shorten revenue cycles, reduce lost charges and denials, prevent underpayments and optimize performance across the enterprise.

Built from the ground up to take advantage of web-based technology, Centricity RIS-IC and various modules enable care across the healthcare IT spectrum to manage radiology information and workflow needs of organizations of different sizes, type, and complexity. Capabilities include:

- **Centricity Precision Reporting** – Leverages Advanced Speech Understanding to efficiently and effectively create diagnostic reports by comprehending the Radiologist’s meaning, not just the spoken word. Creates reports faster and with better accuracy.
- **Patient Self Service** – Enables patients to take control of the registration process and streamlines co-pay charge capture.
- **Electronic Forms** – Take the paper out of the Radiology workflow and enable technologists to capture information in a totally paperless environment.
- **Streamline Workflow** – Documentation available at the appropriate time for the appropriate people.
- **Customized Role-based Work Lists** – Streamline tasks quickly and easily.
- **Third-Party Integration** – Integration with many commercially available PACS systems for streamlined workflow; integration with other 3rd party reporting solutions.

Centricity RIS-IC technology leverages web-based technology to deliver improved radiology informatics and workflow tools to those who need them most. Centricity RIS-IC also is designed to scale, to address the needs of a small facility, as well as the largest of enterprises. Figure 1 provides an illustration of the Centricity RIS-IC solution architecture.
**GE Centricity RIS-IC Solutions with VMware Site Recovery Manager**

![Diagram of Centricity RIS-IC Solution Architecture](image)

**Centricity RIS-IC Solution Components:**

- **Report Server** — hosts reporting via Crystal Reports and provides printing faxing, and bar coding services.
- **Database Server** — RIS-IC Database.
- **ConnectR server** — HL7 & PACS Connectivity, plus hosts the ConnectR product SQL Server-based relational database.
- **Web Server** — Hosts end-user web interface for RIS-IC and Imaging applications.
- **Active Directory / DNS** — Microsoft Active Directory (Domain Controller).

**NOTE:** For more information on GE Centricity RIS-IC, and its module features and functionality, go to the product detail web page for GE Centricity RIS-IC.

The scope of the solution described in this document is based on a VMware lab validation to demonstrate the key concepts of Disaster Recovery utilizing VMware Site Recovery Manager and includes the GE Centricity RIS-IC application. The deployment environment includes:

- Installation and configuration of GE Centricity RIS-IC on VMware vSphere™.
- Storage array technology used to replicate LUNs synchronously and asynchronously between a primary and secondary site.
- Setup of protection group and recovery plans in VMware Site Recovery Manager.
- Execution of non-disruptive test of recovery plan.
- Execution of a true failover of the application with subsequent testing of the application functionality.

In this document, we refer to two datacenter sites called "primary" and "secondary". VMware also refers to these as "protected" and "recovery" sites. 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).
VMware Site Recovery Manager

VMware Site Recovery Manager is a disaster recovery management and automation solution for the VMware platform. 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 recovery plans. Site Recovery Manager integrates tightly with VMware vSphere, 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 2 depicts the technical architecture of Site Recovery Manager with storage array replication across two sites.

Site Recovery Manager is a plug-in to VMware vCenter, so disaster recovery tasks can be executed from the same centralized interface that is used to manage other virtual machine administrative tasks such as creation, migration, and deletion. 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, both Site Recovery Manager and vCenter data repositories can be created 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 document lists the storage replication adapters currently supported by VMware and its storage partners for use with Site Recovery Manager 4.0 and prior versions 1.0 and 1.0 Update 1:


**Site Recovery Use Cases**

While VMware Site Recovery Manager is touted as a “disaster recovery management and automation solution”, there are other situations when SRM can be leveraged to provide High Availability and Business Continuity in scenarios when a true “disaster” has not occurred. Some of these scenarios include planned or unplanned extended power outages. While not considered a true “disaster”, in a hospital environment, an extended power outage could result in a patient care disaster. SRM can be utilized in this scenario to quickly and effectively bring mission-critical services back online.

A second great use case for SRM is a Datacenter Evacuation, again planned or unplanned. Perhaps, as part of their DR plan, a site requires a planned failover to a secondary site. Using SRM, this failover to a secondary site can first be tested and then executed/failed over in a very short period of time.

A third very important use case is a Datacenter Migration. Leveraging SAN replication and SRM technology, a Datacenter Migration can be done with minimal downtime.

**Solution Design and Setup**

**Solution Architecture**

Figure 3 below shows the virtual architectural design of the GE Centricity RIS-IC solution described in this document. Disaster recovery testing with Site Recovery Manager requires that the virtual machines in the secondary site start from storage that is a snapshot of the target LUNs (on secondary site). This practice ensures the test is run against a storage infrastructure that is isolated from the production environment.
Key points about this setup:

- Site Recovery Manager requires two vCenter servers - one each at the primary and secondary sites. For this validation (built in two labs separated by 12 miles), the vCenter servers were running in virtual machines.
  
  **Note:** Best practice is to virtualize vCenter servers so they can take advantage of VMware vMotion, HA and DRS.

- For data replication, synchronous/asynchronous mode was configured to replicate all the related LUNs from primary to secondary site on EMC and NetApp respectively.
  
  - Synchronous replication is the preferred SAN replication strategy for mission-critical data as there is less likelihood for data loss between sites.
  
  - Asynchronous replication is also supported with the understanding that there may be a delta between data at the protection and recovery site. Contact SAN vendor for additional information regarding asynchronous replication deltas.

- The Storage Replication Adapter (SRA) was installed on the primary and secondary vCenter servers. The SRA:
  
  - 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 VMFS storage.
Physical and Virtual Hardware and Software

Physical Hardware

Table 1 provides a description of the physical infrastructure hardware.

Table 1. Site Recovery Hardware and SAN Specification

<table>
<thead>
<tr>
<th>Hardware Specification</th>
<th>Primary Site</th>
<th>Recovery Site</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ESX Hosts</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 x HP ProLiant BL 480c G1</td>
<td></td>
<td>Dell PE 2950</td>
</tr>
<tr>
<td>Intel Xeon E 5450 @ 3.00 Ghz</td>
<td></td>
<td>Dual Quad Core</td>
</tr>
<tr>
<td>Dual Quad Core</td>
<td></td>
<td>Intel Xeon E 5450 @ 2.33 Ghz</td>
</tr>
<tr>
<td><strong>SAN</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMC Clariion and NetApp for synchronous and asynchronous operation, respectively</td>
<td></td>
<td>RAID 5 and RAID DP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>500 GB LUN</td>
</tr>
</tbody>
</table>

Installed Software

Table 2 lists the software used in the GE Centricity RIS-IC solution.

Table 2. Software Installed for Site Recovery Implementation

<table>
<thead>
<tr>
<th>Installed Software</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware</td>
<td>VMware vSphere 4.0, vCenter Server 4.0, ESX® 4.0, Site Recovery Manager 4.0</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Microsoft SQL Server 2005</td>
</tr>
<tr>
<td>GE</td>
<td>GE Centricity RIS-IC, V10.6.0.999 Update 7</td>
</tr>
</tbody>
</table>
Virtual Machine Configurations

Table 3 lists the configuration of virtual machines used to implement the GE Centricity RIS-IC solution on VMware virtual infrastructure.

Table 3. Site Recovery Virtual Machine Specification

<table>
<thead>
<tr>
<th>Virtual Machines</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>2vCPU</td>
</tr>
<tr>
<td></td>
<td>2 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Windows 2003 SP2</td>
</tr>
<tr>
<td>GE ConnectR</td>
<td>4 vCPU</td>
</tr>
<tr>
<td></td>
<td>4 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Windows 2003 SP2</td>
</tr>
<tr>
<td>GE Database Server</td>
<td>4 vCPU</td>
</tr>
<tr>
<td></td>
<td>8 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Windows 2003 SP2</td>
</tr>
<tr>
<td>GE Report Server</td>
<td>4 vCPU</td>
</tr>
<tr>
<td></td>
<td>4 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Windows 2003 SP2</td>
</tr>
<tr>
<td>GE WebServer</td>
<td>2 vCPU</td>
</tr>
<tr>
<td></td>
<td>3 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Windows 2003 SP2</td>
</tr>
</tbody>
</table>

Figure 4 shows the virtual machines in the vCenter display.
Solution Configuration Steps

The hardware and software for the GE Centricity RIS-IC virtualized solution was installed and configured in the following order:

1. Configure storage arrays at the primary and secondary sites.
2. Create LUNs on the primary site storage and expose to primary site ESX host server.
3. Configure storage replication between primary and secondary site storage arrays.
4. Install vCenter Server 4.0 on two Windows virtual machines. These virtual machines will serve as primary and secondary site vCenter Server instances.
5. Install and configure Site Recovery Manager on the primary and secondary vCenter Server instances. (See the next section for details.) Site Recovery Manager can be installed as a separate standalone virtual machine or you can use the same database server to support the vCenter database instance and the Site Recovery Manager database instance.
6. Install GE RIS-IC virtual machines on the primary site.
GE Centricity RIS-IC Solutions with VMware Site Recovery Manager

VMware SRM Installation and Configuration

The following section provides a high level overview of Site Recovery Manager installation and configuration. For detailed configuration information, refer to Appendix A.

Primary and Secondary Site

- Install SRM server at the protection and recovery site. In this test scenario, SRM was installed on the vCenter server.
  
  **Note:** Other install options are available. Site Recovery Manager can be installed as a separate standalone virtual machine or on the same database server as the vCenter database instance.
- Install the Site Recovery Manager Plug-in into vCenter.
- Install the Storage Replication Adapters on the SRM server at each site.

After installation, the Site Recovery Manager plug-in is available and can be accessed via the vSphere or VMware Infrastructure (VI) Client. The primary vCenter Server display, as shown below, lists the configuration steps required after the initial installation.

![SRM Screenshot of Summary Tab (Primary Site)](image)

As shown above, execute the following configuration steps to configure Site Recovery Manager.

**Primary Site**

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

- Create the recovery plan "GE_RG".
  
  The option is available, when creating a recovery plan, to suspend non-critical virtual machines that are running at the secondary site. Typically, the hardware on the secondary site can be used to host virtual machines, so it is not idle.

- Prioritize the virtual machines start order as required.
  
  Options are available to:
  
  - Create a customization specification for the virtual machines so that they start up on the secondary site on a different subnet from the primary site.
  
  - Perform no custom specification and configure virtual machines to start up in a private test “bubble” network using the same networking parameters as the primary site.

Disaster Recovery Testing

Disaster recovery testing comprises development and testing of a logistical plan for how an organization will recover and restore partial or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption. This logistical plan is commonly referred to as a Business Continuity Plan. The old saying goes 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 enough; the result being an insurance policy that does not pay off when you really need it.

Disaster recovery testing is often difficult to perform because it is can be very disruptive, expensive (in terms of resources necessary to carry out), and because disaster recovery plans may be extremely complex. By leveraging virtualization, Site Recovery Manager can help address these problems. Site Recovery Manager has the ability to recover virtual machines and network connections that can be tested as “walled-off” virtual entities — perhaps even co-resident with production applications that might be running at the remote site. This ability to logically encapsulate and test a complete recovery scenario in a set of virtual machines provides a huge simplification of the task and can save significant time and resources.

Using Site Recover Manager, you can 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 recovery 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 server, the automatically-generated test bubble network connects the virtual machines together via a private virtual switch (to prevent interference with the secondary site network) and traffic does not leave that switch. 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 is to use an isolated VLAN, which is documented at:


  - The other option, instead of creating a test bubble, is 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. While we are discussing options for a recovery test, network customization settings would be used for actual recovery. 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 respectively at:

The test bubble scenario and the actual recovery test were chosen for the recovery test described in this document. Configuration steps are detailed in Appendix A.

**Execute Recovery Plan Test**

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

- Start Site Recovery Manager (SRM) disaster recovery test on secondary site for recovery plan "GE_RG".
- During the recovery test, SRM will start the virtual machines defined in the recovery plan and then stop and wait for user input before performing a cleanup and removal of the recovered virtual machines and storage. Figure 6 provides an illustration of this process.
- The virtual machines defined in the recovery plan are up and running in vCenter and can be accessed for user testing. As per the design described in this example, the virtual machines are started up in a test bubble network that uses the same network parameters as in the primary site. Figure 7 shows the virtual machines migrated on the recovery site with no other changes.
- Once the Recovery Plan test completes, click Continue from VI Client recovery display to ensure proper cleanup.

![Figure 6. Recovery Plan Steps during Test Recovery of GE RIS Virtual Machines (Secondary Site)](image)

![Figure 7. Virtual machines of the recovery site on a test bubble network (Secondary Site)](image)
GE Centricity RIS-IC Solutions with VMware Site Recovery Manager

The GE Centricity RIS-IC application can be tested within this network bubble and virtual machines can communicate with each other, but not with any entity outside of this bubble.

- The first test involved configuring a local printer on the guest virtual machine. At the application layer, settings were configured to allow Centricity RIS-IC to see this printer whenever the command is fired. We then successfully tested the setup by sending a print command to the local printer before triggering failover. After failover, the printer configuration settings and guest level printer settings are confirmed and printing is successful.

- The second test case involves inserting an entry in the database that is reflected in the user interface of the application. The objective was to validate data integrity, and verify there is no data loss. After failover, the entry was present in the database, so the test was successful.

- The third test case involves executing a SQL procedure from the DB and validating data integrity by comparing table count results before and after the failover. This test was also successful.

Once the testing is complete, the history of the recovery plan test is saved in SRM, which captures the details of each recovery step. (This information can be used for auditing purposes.) The display below shows the beginning of the report. (The complete output is not shown.)

![Figure 8. History of Recovery Plan Test (Secondary Site)](image)

**Recovery Plan Execution During Actual Failover**

Running an actual recovery plan starts the virtual machines on the secondary site on the secondary site network. This process cannot be undone automatically and will permanently alter 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, no action is taken by SRM 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; this process is covered in more detail in the VMware Site Recovery Manager Administration Guide:


General Recommendations

Based on test results, here is a list of recommendations to achieve the best performance in implementing site recovery solutions:

• It is recommended that Site Recovery Manager database be installed as close to the Site Recovery Manager server as possible – such that it reduces the round trip time (RTT) between both of them. That way, the impact of round trips to the database server on recovery time performance will be reduced. You can use the same database server to support the vCenter database instance and the Site Recovery Manager database instance.

• Grouping virtual machines under fewer protection groups enables faster test and real recoveries, provided those virtual machines have no constraints preventing them from being grouped under similar protection groups.

• It is a good practice to have VMware DRS enabled on a recovery site. Migrations might occur as VMware DRS tries to load balance the cluster during the recovery.

• It is a good practice to enable DPM on recovery site clusters if your recovery site hosts are in the standby state. More hosts lead to increased concurrency for recovering virtual machines and thus results in shorter recovery time. If DPM is not enabled, and the hosts are in a standby state, bring the hosts out of standby mode manually and drag and drop shadow virtual machines on them.

• It is important to chart out the dependencies between virtual machines and define recovery priorities, so that only a certain number of required virtual machines will be assigned as High priority. It is important to note that High Priority protection groups will power up virtual machines sequentially, while Medium and Low protection groups will power up virtual machines in parallel. Assign virtual machines to the appropriate protection groups to reduce overall failover times. As an alternative to placing virtual machines in a High priority group, one can separate all the virtual machines to be recovered in 2 logical groups – Group1 with level 1 virtual machines and Group2 with level 2 virtual machines (which are dependent upon virtual machines in Group1). Group1 virtual machines can then be placed in the normal priority group and Group2 virtual machines in the low priority group within the same plan. This should maintain dependency across both logical groups and will still reduce the recovery time by introducing more concurrency for both priority groups. Note that dependency is maintained between priority groups and there is no concept of dependency across virtual machines within a single priority group.

• It is strongly recommended that VMware Tools be installed in all protected virtual machines so you can accurately acquire their heartbeats and network change notification.

• Make sure any internal script or call-out prompt does not block recovery indefinitely.

• Specify a non-replicated datastore for swap files. This avoids wasting network bandwidth during replication between two sites and remote calls to vCenter Server (during a recovery to delete swap files for all virtual machines), which in turn helps in speeding up the recovery.

• VMware recommends a minimum of two hosts at a recovery site. While not a requirement, having two hosts ensures availability for VMware services at the recovery site; including VMware vMotion, HA and DRS, and will improve recovery time.

• VMware SRM relies on the underlying storage capabilities to failover from protection to the recovery site. Recovery time can vary depending upon the san vendor, replication type, etc. It can take 5-10 minutes to make the changes to back-end storage. Following VMware best practices for SRM, along with SAN vendor best practices, will ensure optimal recovery time.
Summary

This document demonstrates how VMware Site Recovery Manager enables the design of an effective and automated disaster recovery solution using the example of a multi-tier GE Centricity RIS application deployed on VMware virtual infrastructure. Using Site Recovery Manager for this solution lets you:

- Accelerate recovery for the virtual environment through automation. The recovery of GE 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 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. Working with 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.

Additional Resources

VMware Reference Documents and Web sites

- VMware Site Recovery Manager 14.0 Release Notes: http://www.vmware.com/support/srm/srm_10_releasenotes.html

GE Reference Documents and Web Sites

- GE Main Site Links: https://www2.gehealthcare.com/portal/site/usen/
- GE Centricity RIS-IC Links: https://www2.gehealthcare.com/portal/site/usen/ProductDetail/?vgnextoid=5df2bf371de30210VgnVCM10000024dd1403RCRD&productid=4df2bf371de30210VgnVCM10000024dd1403
Appendix A: Site Recovery Manager Setup

Configure Storage Array Manager (Primary Site)

The storage array manager is configured on the primary site vCenter using Site Recovery Manager and clicking **Array Managers**.

**NOTE**: This appendix does not show all the steps in the setup process.

During the configuration process, SRM will automatically detect the datastores that are being replicated and display them in the configuration wizard as shown below.

![Figure 9. Array Managers Configuration](image)

Configure Inventory Mappings (Primary Site)

Configuring inventory preferences provides mappings between compute resources, virtual machine folders, and networks on the primary site and their counterparts on the secondary site as shown below.
Figure 10. Mapping between resources on the protected and recovery sites

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 side. This placeholder virtual machine, sometimes referred to as a recovery virtual machine, is 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 screens show portions of the process used to create a protection group in Site Recovery Manager.
The datastore with the GE Healthcare virtual machines is assigned to the protection group as shown below.
On the secondary site, assign a LUN location to the placeholder configuration files of the protected virtual machines as shown below.

![Datastore for Placeholder VMs](image)

*Figure 13. Placeholder for virtual machine configuration files*

The resulting protection group is shown below.

![Site Recovery Protection Groups and Recovery Plans](image)

*Figure 14. Site Recovery Protection Groups and Recovery Plans*

**Create Recovery Plan (Secondary Site)**

Use the Recovery Plan Wizard prompts in Site Recovery Manager to create a plan name and assign the protection groups 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 in the following sequence of screen shots. Figure 15 below shows how the "GE_PG" protection group is assigned to the plan. All the virtual machines defined in the "GE_PG" protection group are now automatically included into the recovery plan.
Figure 15. Assign the protection group while creating the recovery plan.

Figure 16 shows where the recovery network is specified. In this example, we chose "Auto" and "VM Network", which means the virtual machines are recovered into a test bubble network and to the main network on the secondary site, respectively.

Figure 16. Selecting the port group for the failover virtual machines
The resulting recovery plan is shown below.

Figure 17. GE_RG Recovery Plan

From the previous display, it is possible to assign a guest customization to each virtual machine; select the virtual machine and click Edit... From the display that appears, you can assign a pre-defined custom specification.

Figure 18. Customization specification wizard for automatic assignment of network topologies to the failover virtual machines

The custom specification has to be created before assignment to the virtual machine. This can be done by invoking the Customization Specification Manager on the secondary Site Recovery Manager Server site (from the VI Client, select Edit > Customization Specifications). This opens the Guest Customization Wizard in which the secondary/recovery site network parameters can be defined as shown in the screenshot below.
Figure 19. Summary of the Customization specification contents

Configuring guest customizations for multiple virtual machines can be automated as described in the following papers, "Automating Network Setting Changes" and "DNS Updates on Recovery Site Using VMware vCenter Site Recovery Manager", available respectively at:


These papers demonstrate:

- 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.