



# FujiFilm DR to the Cloud using VMware vSphere Replication 5.0

December 2012

DEPLOYMENT AND TECHNICAL CONSIDERATIONS GUIDE

## Table of Contents

<b>Introduction</b> .....	<b>1</b>
<b>Executive Summary</b> .....	<b>1</b>
<b>VMware and FujiFilm Overview</b> .....	<b>4</b>
FujiFilm Suite Overview .....	4
Foundation Technologies .....	4
VMware Virtual Infrastructure .....	5
<b>VMware Site Recovery Manager with vSphere Replication</b> .....	<b>6</b>
FujiFilm Architecture and Deployment .....	6
FujiFilm Managed Services Modules .....	7
FujiFilm Test Process and Results .....	8
Hardware and Software Configuration .....	8
Installed Software .....	9
Virtual Machine Configuration .....	10
Shared Site Configuration .....	11
vSphere Replication Limitations .....	13
Network Recommendations .....	13
Security Recommendations .....	13
Failback .....	14
<b>Technical Support</b> .....	<b>15</b>
<b>Conclusions</b> .....	<b>15</b>
<b>Resources</b> .....	<b>15</b>
<b>Acknowledgements</b> .....	<b>15</b>

## Introduction

Virtualization is rapidly transforming the IT landscape and fundamentally changing the way that people compute. Today's powerful x86 computer hardware was originally designed to run only a single OS. This approach introduced a tight coupling between the Operating System (OS) and hardware. Virtualization breaks that bond between the two by making it possible to run multiple OS and applications on the same computer at the same time, increasing the utilization and flexibility of hardware.

This document describes DR to the cloud solution for a virtualized FujiFilm Synapse application configured with VMware @Site Recovery Manager (SRM) using vSphere Replication.

Companies that have deployed the FujiFilm Synapse 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 Host based vSphere replication to provide an effective availability solution for mission-critical FujiFilm Synapse deployments.

VMware vCenter™ Site Recovery Manager (SRM) 5.0 is part of the VMware vCenter family of management products. SRM enables you to build, manage, test and execute reliable disaster recovery plans for your VMware virtual environment. The goal of this exercise is to test the Disaster Recovery to the cloud using VMware vSphere Replication with the FujiFilm Synapse application. VMware's Disaster Recovery to the Cloud Services make disaster recovery broadly accessible for all applications and sites by providing cost-efficient, automated and simple disaster protection.

## Executive Summary

VMware vCenter™ Site Recovery Manager (Site Recovery Manager) is the premier tool to enable you to build, manage and execute reliable disaster recovery plans for your virtual environment. Taking full advantage of the encapsulation and isolation of virtual machines, Site Recovery Manager enables simplified automation of disaster recovery. It helps meet recovery time objectives (RTOs), reduces costs traditionally associated with business continuance plans and achieves low-risk and predictable results for recovery of a virtual environment.

The primary goal of this validation was to test failover of the FujiFilm Synapse Application Suite using VMware vSphere Replication across 2 sites with the primary site in Denver and Recovery site in Florida.

Following are the different phases of testing:

### Phase I

- Build the Disaster Recovery setup on both sites using VMware SRM 5.0(vSphere Replication).
- Test if the FujiFilm Synapse Product Suite's virtual machine(s) replicate successfully from Protected Site to the Recovery site.

### Phase 2

- Test the failover of the FujiFilm Synapse Product Suite's VM's and make sure they come up cleanly on the Recovery site.
- Test all the functionalities of the Suite work as expected

### Phase 3

- Test the multi tenancy site security using the vCenter Roles and Privileges.
- Create users with different roles and test the permissions to access different objects

## VMware and FujiFilm Overview

VMware (NYSE:VMW), the global leader in virtualization and cloud infrastructure, delivers customer-proven solutions that accelerate IT by reducing complexity and enabling more flexible, agile service delivery. VMware enables enterprises to adopt a cloud model that addresses their unique business challenges. VMware's approach accelerates the transition to cloud computing while preserving existing investments and improving security and control. With more than 300,000 customers and 25,000 partners, VMware solutions help organizations of all sizes to lower costs, increase business agility and ensure freedom of choice.

### FujiFilm Suite Overview

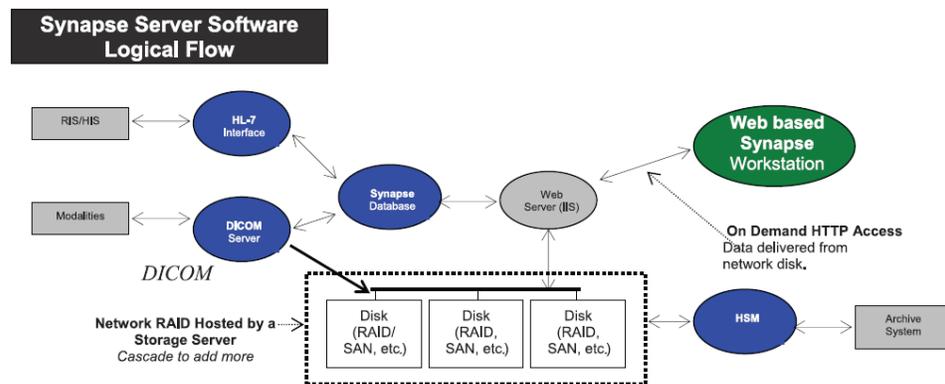


Figure 1: FujiFilm Suite Overview

### Foundation Technologies

Synapse is a collection of software modules built on the Microsoft® Windows® Server platform and workstation software on Windows Workstation editions, which together provide the core software functionality for Synapse – Fuji Film film's Next Generation PACS.

Server modules work with the workstation software to provide powerful foundation technologies to serve the radiology department, the healthcare enterprise and beyond. These multi-site authentications, comparison access and network utilization technologies include products such as MultiView, CommonView, DICOM SCU, AONTM (Access Over Network) Compression, AON Subscription and AON Recollection.

For more information on foundation technologies, visit:  
<http://www.FujiFilmfilmusa.com/shared/bin/foundation.pdf>

## VMware Virtual Infrastructure

VMware's leading virtualization solutions provide multiple benefits to IT administrators and users. VMware virtualization creates a layer of abstraction between the resources required by an application and operating system, and the underlying hardware that provides those resources. A summary of the value of this abstraction layer includes the following:

- **Consolidation:** VMware technology allows multiple application servers to be consolidated onto one physical server, with little or no decrease in overall performance.
- **Ease of Provisioning:** VMware virtualization encapsulates an application into an image that can be duplicated or moved, greatly reducing the cost of application provisioning and deployment.
- **Manageability:** Virtual machines may be moved from server to server with no downtime using VMware vMotion™, which simplifies common operations like hardware maintenance and reduces planned downtime.
- **Availability:** Unplanned downtime can be reduced and higher service levels can be provided to an application. VMware High Availability (HA) ensures that in the case of an unplanned hardware failure, any affected virtual machines are restarted on another host in a VMware cluster.

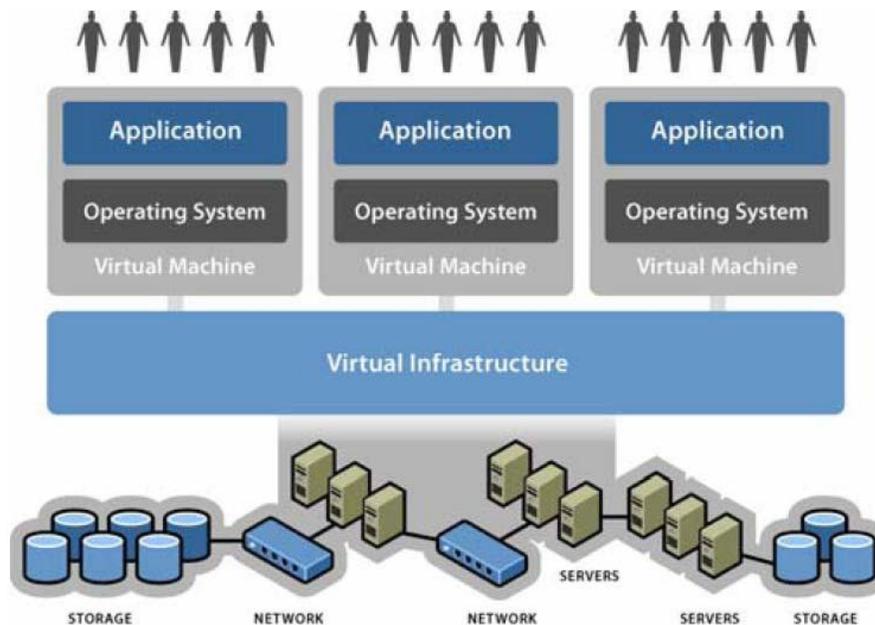
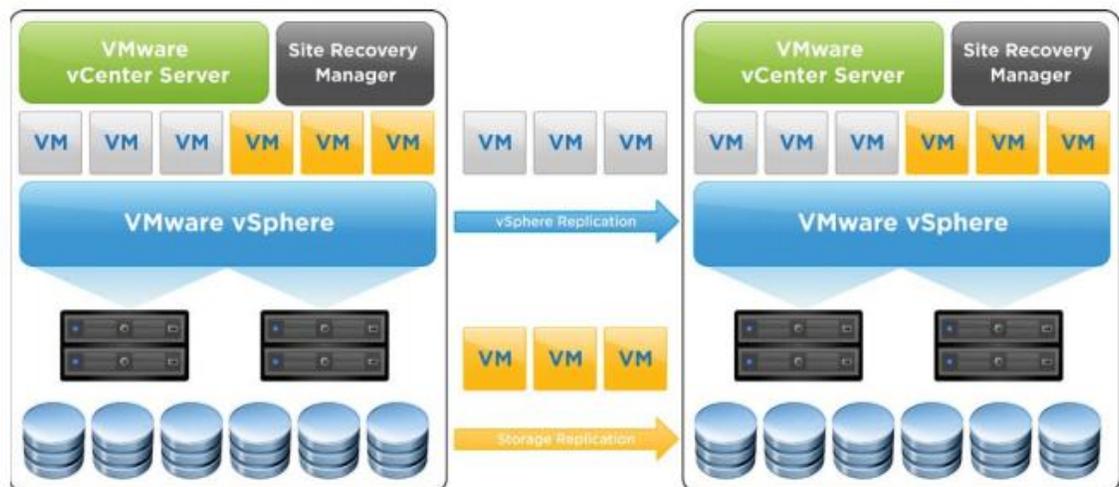


Figure 2: VMware vSphere Virtual Infrastructure

## VMware Site Recovery Manager with vSphere Replication

VMware Site Recovery Manager using vSphere Replication 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™, 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

In vSphere Replication (VR), SRM uses vSphere replication technologies to replicate data to servers at the recovery site. vSphere Replication uses vSphere Replication Management Server (VRMS) to manage the VR infrastructure. VR requires installing the VR Server (VRS) virtual appliance and VRMS virtual appliance, both of which can be installed with SRM during the installation process. While VR does not require storage arrays, an VR storage replication source and target can be any regular storage device, including, but not limited to, storage arrays.



### FujiFilm Architecture and Deployment

Figure 3: FujiFilm Architecture

The FujiFilm Architecture utilizes Microsoft Windows Server platforms deployed in several modules designed to service its foundational product technologies. Each module is designed to perform specific functions and can be combined in single server deployments, or spread between multiple servers; depending on the size and volume of the customer. The modules are explained in more detail below:

## FujiFilm Managed Services 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 11g as its database foundation. At least one logical copy of the database exists in the PACS. For enterprise deployments requiring separate physical databases, multiple logical databases can be deployed and coexist. A user's system access and privileges are all controlled by assignment of database access rights. For high availability requirements, the Synapse Database can be clustered on multiple servers using Oracle Failsafe software and Windows Clustering.

### Web Server

Synapse uses Windows Internet Information Server (IIS) as its core web server. Synapse is a truly web-based system – all data going to and from the Synapse workstation goes through the web server(s). All images, information and user authentication is sent over standard web ports – port 80 for standard communication and port 8080 for SSL are typical in most installations. A special web server called the CodeBase server provides installation files and automatic code update notifications for the Synapse workstation. For enterprise distribution of MultiView and CommonView datasources, the CodeBase server can publish settings for other available datasources and settings. The web server can run on one multifunction server or on multiple servers depending on image volume, available bandwidth and desired functionality.

### 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 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. DICOMServer writes images to standard NTFS file locations and inserts an entry for each image into the Synapse Database as a Uniform Resource Locator (URL). From there, the Synapse Database maintains the image locations for on-demand delivery to workstations. When images are requested, they are streamed directly from the storage system. Upon receipt of images from a modality, a technology called AON™ (Access Over Network) Engine enables DICOMServer Software to generate multiple image versions at varying levels of compression. The AON Engine can write JPEG Lossless and FujiFilmWavelet Lossy image files at user selectable levels of compression based on body part, modality type or a modality's specific AE-Title. DICOMServer can run on one multifunction server or on multiple servers depending on image volume, available bandwidth and desired functionality.

### HIIS Server

The HIIS (Hospital Information Interface) Synapse RIS/HIS 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. As with most Synapse components, the Synapse RIS/HIS Interface Software can run on a single multi-function server system or on one server in a multi-server system. A bi-directional version of HIIS supports study and image notification back to the HIS/RIS and EMR systems for better coordinated enterprise workflow and information sharing.

## FujiFilm Test Process and Results

In this exercise, VMware worked with FujiFilm to test DR to the cloud using the FujiFilm foundational technologies deployed with VMware vSphere Replication

The primary objectives of this testing was to validate that all modules work resiliently on the Recovery site after the failover using VMware vSphere Replication. The joint tests were also designed to provide answers to a common set of questions, and to derive and document a set of best practices that can be used by our customers.

Specifically, key areas under investigation were:

- Successful failover of the Synapse VM to the recovery site.
- Test if all the features of Synapse VM work as expected.
- Test Multitenancy by introducing multiple SRM Instances on Protected and Recovery Site.
- Test Database Consistency and Integrity on the Recovery Site after failback
- Test replication performance based on RPOs and RTOs
- Test fail-over and fail-back procedures and processes including network remapping for product recovery, integrity and availability requirements

### **Phase 1 Result:**

Initial replication over WAN link successful. Took approximately 4 hours with base installation. This will vary depending on size of environment, bandwidth, etc.

### **Phase 2 Result:**

Initial setting of Recovery Point Objective (RPO) at 15 minutes appeared to be sufficient for amount of data being replicated. Again this will be dependent upon environment, amount of data, and bandwidth. Initial failover took less than 15 minutes to complete. Environment powered on successfully based on SRM configuration. All Synapse services, database etc. all started and working as expected, Synapse environment up and running after failover. Image retrieval from Synapse client connected to Recovery Site successful.

### **Phase 3 Result:**

Multi-tenancy for 3 sites configured and appropriate security settings enabled for 3 separate protected sites configured within protected site SRM instance following guidelines in Installing, Configuring, and Using Shared Recovery Site Support. <https://www.vmware.com/pdf/srm-shared-recovery-50.pdf>

Successfully tested isolation of resources across different users using vCenter Roles and permissions. Created new user roles with restrictions on various options like folders and associate users with these roles. Tested logging in with user1 and was able see datastores associated only with user1. Tested isolation with different components of vSphere like Networking, Datastores & Clusters and VM & Templates.

## Hardware and Software Configuration

The following table describes the configuration of ESX host servers and storage in the FujiFilm test configurations.

HARDWARE	CONFIGURATION
HP Proliant BL460c G6 (Nehalem Boxes)	<p>Two HP Proliant BL 460c G6 servers. Each server is equipped with:</p> <ul style="list-style-type: none"> <li>• Intel(R) Xeon(R) Nehalem CPU X5560 2.80 GHz</li> <li>• Sockets: 2</li> <li>• Number of Cores per Socket: 4</li> <li>• Hyper threading: Enabled</li> <li>• 48 GB RAM</li> <li>• 4 X 1 GB NICS per ESX host</li> <li>• Local SAS Storage</li> </ul>

Table 1: ESX Host Hardware

### Installed Software

Table 2 lists the software used for the FujiFilm solution running on VMware virtual infrastructure.

INSTALLED SOFTWARE	
VMware	VMware vSphere ESX 5.0.0 (vSphere) Build 469512
FujiFilm	VMware vSphere ESX 5.0.0 (vSphere) Build 469512

Table 2: Software Installed for FujiFilm Testing on VMware Virtual Infrastructure

## Virtual Machine Configuration

The following table describes the configuration of virtual machines running on ESX host servers in the FujiFilm test configurations.

VIRTUAL MACHINE	HARDWARE CONFIGURATION
vCenter (2 instances for Protected and Recovery)	<ul style="list-style-type: none"> <li>• 2 vcpu</li> <li>• 4 GB</li> <li>• Ethernet card(1 Gbps Network)</li> <li>• Disk storage 1 X 30 GB vmdk only</li> </ul>
SRM (2 instances for Protected and Recovery)	<ul style="list-style-type: none"> <li>• 2 vCPUs</li> <li>• 4 GB</li> <li>• Ethernet card(1 Gbps Network)</li> <li>• Disk storage 1 X 30 GB vmdk only</li> </ul>
VRMS (2 Instances for Protected and Recovery)	<ul style="list-style-type: none"> <li>• 2 vCPU</li> <li>• 4 Gb</li> <li>• Ethernet card(1 Gbps Network)</li> <li>• Disk storage 1 X 10 GB vmdk only</li> </ul>
vSphere Replicator(VRS) – 2 Instances(Protected and Recovery)	<ul style="list-style-type: none"> <li>• 1 vcpu</li> <li>• 512 MB</li> <li>• Ethernet card(1 Gbps Network)</li> <li>• Disk storage 1 X 6 GB vmdk only</li> <li>• Disk storage 1 X 2 GB vmdk only</li> </ul>

**Table 3: Virtual Machine Configuration**

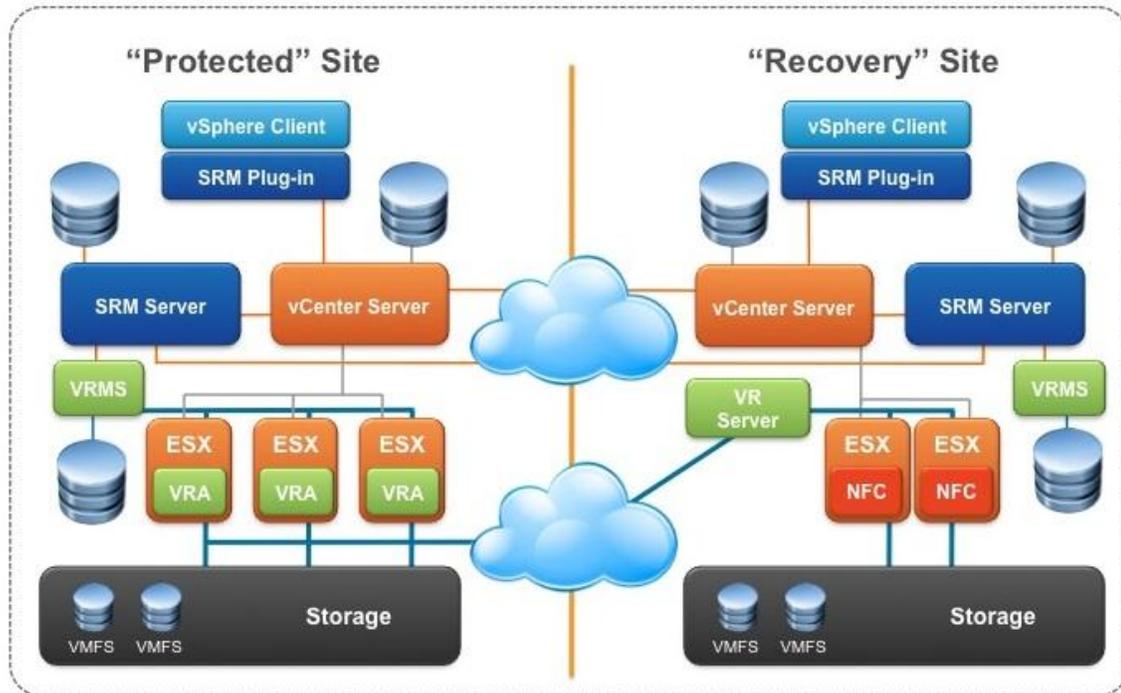


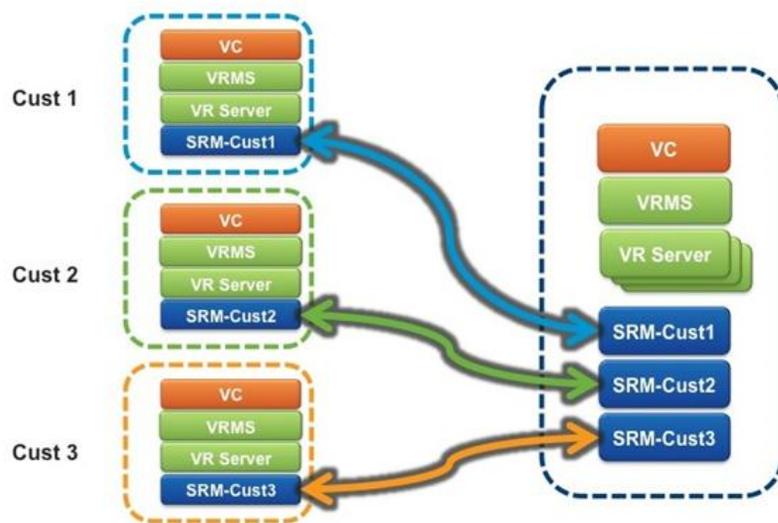
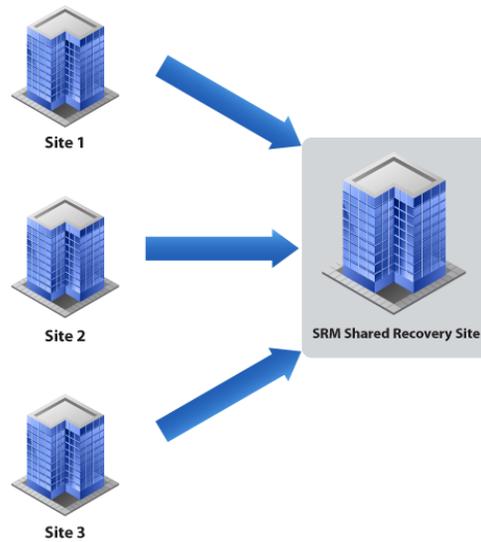
Figure 4: FujiFilm Test Configuration

The above figure shows the virtual architectural design of the FujiFilm Synapse solution described in this document. Disaster recovery testing with Site Recovery Manager requires that the virtual machines to be replicated on to the secondary site start using VMware vSphere replication technology

### Shared Site Configuration

At a shared recovery site, multiple customers share a single vCenter and in some cases a single ESX host. The vCenter administrator at the shared recovery site must manage permissions so that each customer (where customer is defined as the owner of an SRM extension) has sufficient privileges to configure and use SRM, but no customer can access resources that belong to another customer.

When configured for shared recovery site support, SRM supports the same procedures and workflows that it does in the normal configuration.



The above diagrams depict the architecture of the shared site configuration. For each shared recovery site customer, you must install SRM once at the customer site and again at the recovery site. Both installations must specify the same custom SRM extension.

Each SRM server installation at the shared recovery site must have a dedicated host. You cannot install multiple instances of the SRM server on a single host. See the SRM Administration guide at [https://www.vmware.com/pdf/srm\\_admin\\_5\\_0.pdf](https://www.vmware.com/pdf/srm_admin_5_0.pdf) and Shared Recovery Site Support at <https://www.vmware.com/pdf/srm-shared-recovery-50.pdf>

The diagram above shows one important difference between the VRMS pairings and the SRM server pairings. Note how all three customer VRMS appliances are able to establish a unique

paired relationship with the same VRMS appliance. This is possible due to the way in which VMware have built the VRMS appliance. The VRMS appliance is able to manage N:1 connectivity from within itself without the need for the custom extension technique used by the SRM servers.

### vSphere Replication Limitations

With any new feature or functionality there are always limitations. vSphere Replication is no exception to this and yes we have limitations that need to be understood. For the intended use cases and DR protection in general we would not expect any of these to be limiting but it's worth listing them out to start with:

- ISOs and floppy images are not replicated
- Powered-off/suspended VMs are not replicated
- Non-critical files are not replicated (i.e. logs, stats, swap, dumps)
- Snapshots work with vSphere Replication, snapshot is replicated but VM is recovered with snapshots collapsed
- Physical RDM's are not supported
- FT, Linked Clones, VM Templates are not supported
- Automated failback of vSphere Replication protected VM's is not supported in the GA release. Manual failback is required.
- Virtual hardware 7 or later is required for the VM's being protected with vSphere Replication

The limitations above should hopefully be expected and logical though the standout item requiring a bit more explanation is probably the "Automated failback.." limitation.

### Network Recommendations

In addition to the vRS limitations, there are some additional network recommendations that should be noted when configuring vSphere Replication. These are detailed below.

- NAT'd configuration is not supported across the sites because when we configure vSphere Replication the VRMS appliance will write the IP address (not DNS name) of the VR server appliance into the .vmx file of the VM being protected so that the VR Filter know where to send the light weight delta traffic to. As this natted IP address is coming from the target site the replication fails. This issue can be resolved using the site to site vpn wherein all the IP's are accessible.
- "Stretched VLAN" in campus environment or VPN required
- Public IP addressing not recommended due to security (strict firewall src/dest rules)
- IP Addressing / DNS is VERY IMPORTANT – every component must resolve natively from each site
- Ensure firewall ports in vSphere/ESXi are configured correctly
- Follow convention – if using IP addressing, connect everything using IP, VRMS, VRS, etc, or use DNS for every component.
- Ensure connectivity between all components – vCenter to vCenter, SRM, VRMS, VR must all be able to communicate

### Security Recommendations

At a shared recovery site, multiple customers share a single vCenter and in some cases a single ESX host. The vCenter administrator at the shared recovery site must manage permissions so that each customer (where customer is defined as the owner of an SRM extension) has sufficient privileges to configure and use SRM, but no customer can access resources that belong to

another customer. SRM makes extensive use of vCenter roles and permissions and can be configured at a very granular level to ensure security for various SRM activities. Note the requirements in the image below:

vSphere Replication requires users to have specific permissions set for both source and target vCenter objects. For more information see [Site Recovery Manager Administrator's Guide](#).

**Source site permissions required for:**

- vCenter server root folder
- Virtual machine being configured for replication
- Datastores used by the virtual machine

**Target site permissions required for:**

- vCenter server root folder
- Target datastores

---

**Permissions for Site Recovery for Site 1 (Local)**

Permissions for this object are set on the vCenter Server: Recovery.

Some additional considerations are listed below.

- Create separate customer folders in vCenter VMs and Templates View to manage each customer's VMs.
- Create separate storage folders and/or datastores for each customer.
- Create separate SRM users/administrators in AD or vCenter for each customer.
- Optional: Create separate Network vSwitches for each customer and assign unique port groups/VLANs for additional security at the network layer.
- Clone the appropriate SRM role in vCenter and assign to SRM users/administrators.
- Assign the appropriate customer to the appropriate datastore/folder for their site.
  - Depending on requirements, this role can be modified to add or remove rights as necessary. In our testing, we used a clone of the "VRM target datastore user"
- Assign the appropriate SRM customer role to root of vCenter at Recovery site. Remember in vCenter the user needs to "walk the tree", so rights will need to be assigned at the root, datacenter, and cluster level. You will also need to assign specific rights to the SRM instance VM. vSphere Replication Management and vSphere Replication servers can be shared between customer sites.
  - For our testing, we cloned the SRM Recovery Test Administrator role and assigned appropriate users, ensuring each site only had access to their own storage, VMs, and folders.
- Assign the appropriate customer within SRM plugin to Protected and Recovery site. This will be set at the root level when SRM plugin is launched. For our testing we used the SRM Recovery Test Administrator role.

## Failback

SRM 5.0 introduces the ability to automate the failback of VM's that were failed over to the recovery site. Note that the ability to automate failback (a combination of the new reprotect workflow and a failover in the reverse direction) also implies you are failing back to the same datacenter, equipment and configuration you failed over from. With vSphere Replication and SRM 5.0 at GA any VM protected with vSphere Replication will not be able to failback using the automated failback process instead these VMs will need to be failed back manually using the process documented in the SRM Admin Guide

[http://www.vmware.com/pdf/srm\\_admin\\_5\\_0.pdf](http://www.vmware.com/pdf/srm_admin_5_0.pdf) .

## Technical Support

For technical support on virtualization issues, existing FujiFilm customers should use the following contacts:

## Conclusions

Tests conducted during this validation suggest that outstanding performance was observed with the FujiFilm Synapse application. All the features after the failover were working as expected and bandwidth was not found to be a limiting factor.

Overall testing shows that FujiFilm Synapse can be successfully using DR to the cloud with VMware vSphere Replication

## Resources

Customers can find more information about VMware and FujiFilm products using the links listed below.

### *VMware Resources*

- VMware official website:  
<http://www.vmware.com/>  
VMware vCenter Site Recovery Manager 5.0 Release Notes  
[http://www.vmware.com/support/srm/srm\\_releasenotes\\_5\\_0\\_0.html](http://www.vmware.com/support/srm/srm_releasenotes_5_0_0.html)
- VMware vCenter Site Recovery Manager Administration Guide  
[http://www.vmware.com/pdf/srm\\_admin\\_5\\_0.pdf](http://www.vmware.com/pdf/srm_admin_5_0.pdf)
- VMware vCenter Site Recovery Manager Compatibility Matrixes  
[http://www.vmware.com/pdf/srm\\_compat\\_matrix\\_5\\_0.pdf](http://www.vmware.com/pdf/srm_compat_matrix_5_0.pdf)
- VMware vCenter Site Recovery Manager Partner Compatibility Matrix  
[http://www.vmware.com/pdf/srm\\_storage\\_partners.pdf](http://www.vmware.com/pdf/srm_storage_partners.pdf)

## Acknowledgements

The following individuals contributed to the creation of this deployment guide:

- Balayya Kamanboina, ISV Validation Engineer, VMware
- Ray Milot, Technical Evangelist, VMware
- Ryan Edwards, FujiFilm
- David Kleinman, FujiFilm