Building and Protecting vSphere Data Centers Using Site Recovery Manager (SRM)

Ram Santosh Kodeboyina
St. Cloud State University, kora1401@stcloudstate.edu

Follow this and additional works at: http://repository.stcloudstate.edu/msia_etds

Recommended Citation
Building and Protecting vSphere Data Centers

Using Site Recovery Manager (SRM)

by

Ram Santosh Kodeboyina

A Starred Paper
Submitted to the Graduate Faculty
of
St. Cloud State University
in Partial Fulfillment of the Requirements
for the Degree of
Master of Science in Information Assurance

March, 2016

Starred Paper Committee:
Dr. Dennis Guster, Chairperson
Dr. Susantha Herath
Dr. Sneh Kalia
Abstract

With the evolution of cloud computing technology, companies like Amazon, Microsoft, Google, Softlayer, and Rackspace have started providing Infrastructure as a Service, Software as a Service, and Platform as a Service offering to their customers. For these companies, providing a high degree of availability is as important as providing an overall great hosting service. Disaster is always being unpredictable, the destruction caused by it is always worse than expected. Sometimes it ends up with the loose of information, data and records. Disaster can also make services inaccessible for very long time if disaster recovery was not planned properly. This paper focuses on protecting a vSphere virtual datacenter using Site Recovery Manager (SRM). A study says 23% of companies close within one year after the disaster struck. This paper also discusses on how SRM can be a cost effective disaster recovery solution compared to all the recovery solutions available. It will also cover Recovery Point Objective and Recovery Time Objective. The SRM works on two different replication methodologies that is vSphere replication and Array based replications. These technologies used by Site Recovery Manager to protect Tier-1, 2, and 3 applications. The recent study explains that Traditional DR solutions often fail to meet business requirements because they are too expensive, complex and unreliable. Organizations using Site Recovery Manager ensure highly predictable RTOs at a much lower cost and level of complexity. Lower cost for DR. Site Recovery Manager can reduce the operating overhead by 50% by replacing complex manual run books with simple, automated recovery plans that can be tested without disruption. For organizations with an RPO of 15 minutes or higher, vSphere Replication can eliminate up to $10,000 per TB of protected data with storage-based technologies. The combined solution can save over USD $1,100 per protected
virtual machine per year. These calculations were validated by a third-party global research firm. Integration with Virtual SAN reduces the DR footprint through hyper-converged, software-defined storage that runs on any standard x86 platform. Virtual SAN can decrease the total cost of ownership for recovery storage by 50 percent (VMware, n.d.a).
Acknowledgement

The successful completion of this paper could not have been possible without the guidance of my beloved professors, Dr. Dennis Guster and Dr. Susantha Herath. I also would like to thank Professor Sneh Kalia for being part of the committee and finding the time to read my thesis.

I also would like to thank my mother K. Ganga Bhavani, father K V S V Prasad and friends who were with me supporting me the entire way with whatever was needed.
# Table of Contents

<table>
<thead>
<tr>
<th>List of Tables</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of Figures</td>
<td>9</td>
</tr>
</tbody>
</table>

**Chapter**

I. **INTRODUCTION** ................................................................. 10
   - Introduction ..................................................................... 10
   - Problem Statement .......................................................... 11
   - Definition of Terms ....................................................... 11

II. **BACKGROUND AND LITERATURE REVIEW** ............................. 13
    - Virtualization ............................................................... 13
    - vSphere .......................................................................... 13
    - ESXi .............................................................................. 13
    - vCenter Server ............................................................. 14
    - Virtual Networking ......................................................... 14
    - High Availability .......................................................... 15
    - Update Manager ............................................................. 16
    - Site Recovery Manager .................................................. 16
    - Recovery Point Objective .............................................. 16
    - Recovery Time Objective ............................................... 17
    - Site Recovery Manager 5.0 .............................................. 17

III. **METHODOLOGY** ................................................................. 18
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>18</td>
</tr>
<tr>
<td>How It Works</td>
<td>19</td>
</tr>
<tr>
<td>vSphere Replication</td>
<td>20</td>
</tr>
<tr>
<td>Array Based Replication</td>
<td>21</td>
</tr>
<tr>
<td>Planned Migration</td>
<td>22</td>
</tr>
<tr>
<td>Automated Failback</td>
<td>22</td>
</tr>
<tr>
<td>Scalability</td>
<td>22</td>
</tr>
<tr>
<td>Various Disaster Recovery Topologies</td>
<td>23</td>
</tr>
<tr>
<td>Hardware and Software Requirements</td>
<td>23</td>
</tr>
<tr>
<td>vSphere Replication Agent</td>
<td>25</td>
</tr>
<tr>
<td>Inventory Mappings</td>
<td>26</td>
</tr>
<tr>
<td>Resource Mappings</td>
<td>26</td>
</tr>
<tr>
<td>Folder Mappings</td>
<td>26</td>
</tr>
<tr>
<td>High Availability and Disaster Recovery</td>
<td>26</td>
</tr>
<tr>
<td>IV. IMPLEMENTATION</td>
<td>30</td>
</tr>
<tr>
<td>ESXi Installation</td>
<td>30</td>
</tr>
<tr>
<td>Log on to ESXi</td>
<td>33</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>34</td>
</tr>
<tr>
<td>vCenter Server Specification Requirement</td>
<td>36</td>
</tr>
<tr>
<td>vCenter Server Installation</td>
<td>38</td>
</tr>
<tr>
<td>SRM 5 Database Setup Using Microsoft SQL 2008 R2 Express</td>
<td>45</td>
</tr>
<tr>
<td>Chapter</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>V. SITE RECOVERY MANAGER</td>
<td>56</td>
</tr>
<tr>
<td>Site Recovery Manager</td>
<td>56</td>
</tr>
<tr>
<td>Installation of Site Recovery Manager (SRM)</td>
<td>57</td>
</tr>
<tr>
<td>Installing HP SRA for SRM</td>
<td>64</td>
</tr>
<tr>
<td>Pairing Site Recovery Manager Servers</td>
<td>77</td>
</tr>
<tr>
<td>HP SRA Array Manager for SRM</td>
<td>80</td>
</tr>
<tr>
<td>SRM Resource Mappings</td>
<td>88</td>
</tr>
<tr>
<td>SRM Folder Mappings</td>
<td>90</td>
</tr>
<tr>
<td>SRM Network Mappings</td>
<td>92</td>
</tr>
<tr>
<td>SRM Placeholder Datastores</td>
<td>95</td>
</tr>
<tr>
<td>SRM Protection Group Creation</td>
<td>96</td>
</tr>
<tr>
<td>SRM Recovery Plans</td>
<td>98</td>
</tr>
<tr>
<td>SRM Testing and Failback</td>
<td>100</td>
</tr>
<tr>
<td>VI. TIMELINE</td>
<td>105</td>
</tr>
<tr>
<td>VII. CONCLUSION AND FUTURE SCOPE</td>
<td>106</td>
</tr>
<tr>
<td>References</td>
<td>108</td>
</tr>
</tbody>
</table>
# List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Significant Differences between Windows-based and Linux-based vCenter Deployment</td>
<td>35</td>
</tr>
<tr>
<td>2. vCenter Server Specification for Windows</td>
<td>37</td>
</tr>
<tr>
<td>3. vCenter Server Specification for Linux</td>
<td>37</td>
</tr>
<tr>
<td>4. Dates and Description of the Task</td>
<td>105</td>
</tr>
</tbody>
</table>
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>VMware vCenter Server</td>
<td>14</td>
</tr>
<tr>
<td>2.</td>
<td>Distributed Switch</td>
<td>15</td>
</tr>
<tr>
<td>3.</td>
<td>Shared Storage</td>
<td>15</td>
</tr>
<tr>
<td>4.</td>
<td>Replication on High Level</td>
<td>16</td>
</tr>
<tr>
<td>5.</td>
<td>vSphere Replication Mechanism</td>
<td>21</td>
</tr>
<tr>
<td>6.</td>
<td>Array-based Replication</td>
<td>21</td>
</tr>
<tr>
<td>7.</td>
<td>vCenter Site Recovery Manager Scale</td>
<td>22</td>
</tr>
<tr>
<td>8.</td>
<td>High Availability</td>
<td>28</td>
</tr>
<tr>
<td>9.</td>
<td>vCenter Server Architecture</td>
<td>35</td>
</tr>
</tbody>
</table>
Chapter I
INTRODUCTION

Introduction

Protecting a datacenter and the important applications and services it houses is a critical task for every organization. A disaster is any event that halts business activity on a large scale. A disaster, in terms of IT, can be defined as a complete loss of datacenter services for an extended period of time. Individual component failures, host failures, and service interruptions are not considered disasters by this definition.

VMware offers multiple products which allow organizations to reduce downtime caused by disasters and smaller-scale component failures alike. One such product is Site Recovery Manager, which can allow a company to protect its datacenters against natural disasters as well as providing service continuity during planned maintenance of the primary datacenter. Site Recovery Manager offers two ways of protecting a datacenter. One way is vSphere Replication, which works at a host or server virtual machines level and the second at a storage array level.

The first method is better fit for Tier 2 and Tier 3 applications which has some limitations and the second one can be used for protecting Tier 1 which are business critical applications. This paper focuses on building a vSphere datacenter and protecting it from a disaster using Site Recovery Manager. The Key Features and Capabilities of SRM are—it is VM-centric, policy-based storage, and replication. Replicate in flexible topologies, e.g., from external SAN/NAS to Virtual SAN—no need for matching storage at source and target. Provision and manage replication at the VM level—no more replicating LUNs. Define storage policies to be applied at the destination Virtual SAN Datastore while Configuring (VMware, n.d.a).
Top executives say 10 hours to recovery; IT managers say up to 30 hours. Ninety-three percent of business that lost their data center for 10 days went bankrupt within one year. Source and 43% of companies experiencing disasters never re-open, and 29% close within two years. From the above statements we can understand how critical a disaster recovery plan for a datacenter is (Galante, 2009).

**Problem Statement**

Are we prepared for everything, every time? Well this question continuously repeats in every organization. Every organization has their own Sensitive Data, Customer Data, etc., in Terabytes and Petabytes. Because of the fast growing technology and advancements, many organizations want to make sure their business continuity and data security are at very high level. This paper solely focuses on how a robust disaster recovery solution can be built using vSphere or Array based replication and Site Recovery Manager. That will make sure the above required continuity and security is higher in availability.

**Definition of Terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB</td>
<td>Database</td>
</tr>
<tr>
<td>DR</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>DRS</td>
<td>Distributed Recourse Scheduler</td>
</tr>
<tr>
<td>FT</td>
<td>Fault Tolerance</td>
</tr>
<tr>
<td>HA</td>
<td>High Availability</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>MSCS</td>
<td>Microsoft Cluster Service</td>
</tr>
<tr>
<td>RDM</td>
<td>Raw Device Mapping</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>SMP</td>
<td>Symmetric Multi Processing</td>
</tr>
<tr>
<td>SRM</td>
<td>Site Recovery Manager</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign On</td>
</tr>
<tr>
<td>UP</td>
<td>Uni-processing</td>
</tr>
<tr>
<td>vCenter</td>
<td>Virtual Center Server</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual machine</td>
</tr>
<tr>
<td>VR</td>
<td>Virtual Replication</td>
</tr>
</tbody>
</table>
Chapter II
BACKGROUND AND LITERATURE REVIEW

Virtualization

Virtualization is a revolutionary technology that transforms hardware into software and allows building and running multiple operating systems as virtual machines on a single server platform (Raido, n.d.).

Virtualization Benefits

Virtualization benefits include increased performance and increased resource utilization, easier backup and recovery options, greater flexibility and scalability, lower Total Cost of Ownership (TCO) and reduced capital and operational costs.

vSphere

VMware vSphere is a server virtualization product from VMware that allows companies to reduce their capital and operational expenditures. VMware vSphere includes the following technologies; (a) ESXi, (b) vCenter Server, (c) Virtual Networking, (d) High Availability, and (e) Update Manager (VMware, n.d.h).

ESXi

VMware ESXi is a software component which acts as an operating system and enterprise-class hypervisor. ESXi can manage resources from the underlying server hardware and provide them to the virtual machines running on top of it. It facilitates access to the underlying server hardware while ensuring that each VM remains separate from and inaccessible to the others running on the same system (VMware, n.d.d)
vCenter Server

VMware vCenter Server provides centralized administration to vSphere environments. It provides centralized administration of all hosted VMs, as well as additional security and availability features (Gordin, 2015; VMware, n.d.c).

Figure 1. VMware vCenter Server (VMware, n.d.c)

Virtual Networking

A Virtual Distributed Switch (vDS) is created at the datacenter level and acts as a single point of connectivity to all the VMs and other vSphere services present on ESXi hosts (VMware, n.d.f, n.d.j).
Figure 2. Distributed Switch (VMware n.d.e)

High Availability

High Availability (HA) is a vSphere feature which migrates virtual machines from a failed server to healthy server in the same cluster. It provides services continuity and minimizes downtime for virtualized applications.

Figure 3: Shared Storage (Listwon, n.d.)
**Update Manager**

VMware Update Manager is a tool that interacts with vCenter Server, comes as a plugin to vSphere Client, and can be used to patch ESXi servers, virtual machine hardware, and vApps.

**Site Recovery Manager**

Site Recovery Manager is a disaster recovery product from VMware which can be used to create a disaster recovery site for VMware server infrastructures.

![Diagram](image-url)

*Figure 4. Replication on high level. (Mariusz, 2014)*

**Recovery Point Objective**

Recovery Point Objective (RPO) describes the amount of data loss that is deemed acceptable to an organization. The RPO is the point in time to which you must recover data as defined by your organization. This is generally a definition of what an organization determines is an “acceptable loss” in a disaster situation. The RPO allows an organization to define a window of time before a disaster during which data may be lost. The value of the data in this window can
then be weighed against the cost of the additional disaster prevention or loss-prevention
measures that would be necessary to reduce or close the window (VMware White Paper, 2009).

**Recovery Time Objective**

The Recovery Time Objective (RTO) is the duration of time and a service level within
which a business process must be restored after a disaster (or disruption) in order to avoid
unacceptable consequences associated with a break in business continuity. It includes the time
for trying to fix the problem without a recovery, the recovery itself, and communication to the
end users. In accepted business continuity planning methodology, the RTO is established during
the Business Impact Analysis (BIA) by the owner of a process. The RTO attaches to the business
process and not the resources required to support the process (VMware White Paper, 2009).

**Site Recovery Manager 5.0**

VMware vCenter Site Recovery Manager is a business continuity and disaster recovery
solution that helps organizations plan, test, and execute a scheduled migration or emergency
failover of vCenter inventory between sites. SRM relies on data replication mechanisms, such as
array-based or vSphere replication to replicate virtual machines from the protected site to the
recovery site. In the event of a failover, SRM coordinates the recovery process with the
underlying replication mechanism so that the virtual machines at the protected site can be shut
down cleanly (in the event that the virtual machines at the protected site are still available) and
the replicated virtual machines can be powered up. Recovery of protected inventory to the
recovery site is guided by a recovery plan that specifies the order in which virtual machines are
started up (VMware, n.d.g).
Chapter III

METHODOLOGY

Introduction

vSphere Replication duplicates a VMware vSphere infrastructure to an alternate area, inside or in the middle of bunches, and makes that duplicate accessible for reclamation through the VMware vSphere Web Client or through the coordination of a full fiasco recuperation item, for example, VMware vCenter Site Recovery Manager. vSphere Replication secures the virtual machines it protects on a progressive premise. It reproduces to the duplicates just the progressions that are made to the virtual machine. This guarantees that the virtual machine stays secured and is accessible for recuperation from the vSphere Web Client without requiring utilization of an outside apparatus. vSphere Replication is included in all qualified vSphere licenses, extending from VMware vSphere Essentials Plus Kit to VMware vSphere Enterprise Plus Edition. Similarly, as with reinforcements through VMware vSphere Data Protection, securing a virtual machine is a basic capacity of a hypervisor within the datacenter (VMware, n.d.k).

vSphere Replication is managed entirely through components available in the vSphere Web Client. This web-based interface allows centralized administration of all parts of a virtual datacenter, including provisioning, security, and replication tasks. Some replication solutions create unnecessary duplicates of a virtual machine at a remote site without any thought for the consistency of the application data inside the virtual machine. vSphere Replication can help ensure that application and virtual machine data are efficiently and reliably replicated between sites.
How It Works

A solid disaster recovery strategy starts with an array based replication which is the ability to copy the data automatically to a remote site. The result of this is that many storage arrays will have a replication option. This replication option requires one to buy more storage hardware and, hence, most of the vendors provide replication free of cost when you purchase more hardware from them. Copying the data from one location to another is called replication. These copies can be performed at sub-file (block or byte) level wherein the smallest blocks of the data are copied from one site to another and most of the today’s replication products have this ability which allows for an optimal usage of bandwidth. A better solution for the question ‘How to seed and keep a remote DR site up to date?’ would be to make the storage system responsible for the movement of data to a DR site. The array based replication also has some negative effects that need to be considered by storage managers before investing in it. But a point to be noted is that the capacity to clear those comes free with the storage array (Crump, 2011).

Array-based Replication works by replicating storage layer and supports vSphere 3.5 to 6.0, with Recovery Point Objective (RPO) 0 up to max supported by vendor like EMC, NetApp, Dell etc. This scales up to 5,000 VMs protected/2,000 simultaneously recoverable per vCenter/SRM pair and supports write order fidelity within and across multiple VMs in the same consistency group.

The replication takes place at the LUN/VMFS or NFS volume level and can be directly configured on storage array. The major requirement in array base replication is that storage replication solution at both sites (e.g., EMC RecoverPoint, NetApp vFiler, etc.) should be similar. Array based replication supports only FC, iSCSI, or NFS storage and the cost depends
on replication and snapshot licensing. Deployment is fairly involved and must include storage administration and networking. Application consistency may be supported with the addition of agents to the VM, depending on the kind of array.

It can replicate UP FT protected VMs (once recovered VM is no longer FT enabled), but this does not support SMP FT VMs. The most innovative feature of array based replication is it replicates powered off VMs, Templates, Linked Clones (as long as all nodes in the snapshot tree are replicated as well), and ISOs. This methodology supports physical and virtual mode of RDMs, MSCS cluster, and vApps can be replicated and replication process is not obstructed by the host failure (Khalsa, 2015).

**vSphere Replication**

Host-based replication is independent of the underlying storage and it works with a variety of storage types including VMware Virtual SANs, traditional SAN and NAS storage, and direct-attached storage (DAS). Unlike many array replication solutions, vSphere replication enables virtual machine replication between heterogeneous storage types. For example, Virtual SAN to DAS, SAN to NAS, and SAN to Virtual SAN. vSphere replication can, of course, replicate virtual machines between storage targets of the same type, such as Virtual SAN to Virtual SAN (VMware, n.d.m).
Array Based Replication

Array-based replication is a technology that works at a storage array level. It replicates the contents of storage LUNs between associated sites.

Figure 5. vSphere Replication Mechanism (VMware, n.d.1)

Figure 6. Array based Replication (Viltorious, 2015)
Planned Migration

Planned migration is a vCenter Site Recovery Manager workflow that enables application-consistent migration of virtual machine workloads with zero data loss to a recovery site.

Automated Failback

Automated failback provides an automated workflow to migrate virtual machines back to a protected site after it is restored. For obvious reasons, automated failback cannot take place if the protected site is physically lost.

Scalability

Each vCenter Site Recovery Manager Server host supports up to a certain number of virtual machines, protection groups, datastore groups, and concurrent recoveries.

vc

<table>
<thead>
<tr>
<th>Item</th>
<th>Maximums</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Array-Based Replication</td>
</tr>
<tr>
<td>Protected virtual machines in a single protection group</td>
<td>500</td>
</tr>
<tr>
<td>Total protected virtual machines</td>
<td>5,000</td>
</tr>
<tr>
<td>Protection groups per recovery plan</td>
<td>250</td>
</tr>
<tr>
<td>Recovery plans</td>
<td>250</td>
</tr>
<tr>
<td>Datastore groups</td>
<td>255</td>
</tr>
<tr>
<td>Concurrent recoveries</td>
<td>10</td>
</tr>
</tbody>
</table>

Figure 7. vCenter Site Recovery Manager Scale (VMware n.d.n)
Various Disaster Recovery Topologies

- **Active-passive:** vCenter Site Recovery Manager supports the traditional active-passive disaster recovery scenario. In this scenario, a production site that is running applications is recovered at a second site that is idle until failover is required. Although this scenario is most common, it requires paying for a disaster recovery site that is idle most of the time.

- **Active-active:** vCenter Site Recovery Manager enables you to leverage your recovery site for other workloads when you are not using the site for disaster recovery. vCenter Site Recovery Manager can be configured to shut down or suspend virtual machines at the recovery site as part of the failover process. This configuration frees up compute capacity for the workloads being recovered (Finke, 2009).

- **Bi-directional:** vCenter Site Recovery Manager provides bidirectional failover protection so that you can run active production workloads at both sites and fail over to the other site in either direction. The spare capacity at the other site is used to run the virtual machines that are failed over.

- **Shared Recovery:** Shared recovery refers to the capability of recovering multiple protected sites (up to a maximum of 10 sites) to a single disaster recovery site. Shared recovery is useful if you are a disaster recovery provider offering disaster recovery services to remote offices or smaller companies.

**Hardware and Software Requirements**

- Two or more physical servers in each site.

- Two or more ESXi servers: At least one in primary site and one in disaster site.
- Two vCenter servers: one at primary site and one at disaster site.
- Two SRM servers: one at primary site and one at disaster site.
- Two storage arrays capable of array based replication.

**vSphere and vCenter Server Requirements**

- vCenter Server must be installed at both the protected site and the recovery site.
- VMware ESXi versions 4.x through 5.x are supported.
- VMware vSphere Replication requires ESXi 5 or higher.
- vCenter Site Recovery Manager supports the following vSphere Editions:
  - VMware vSphere Standard Edition
  - VMware vSphere Enterprise Edition
  - VMware vSphere Enterprise Plus Edition
  - VMware vSphere Essentials Plus Kit

**vCenter Site Recovery Manager Server Requirements**

VMware vCenter Site Recovery Manager Server is supported on the same Microsoft Windows operating systems as vCenter Server. The software requirements are as follows:

- A 64-bit Windows operating system is required.
- A vCenter Site Recovery Manager Server can be a physical server or a virtual machine.
- A 64-bit database source name (DSN) must be created for connecting to the vCenter Site Recovery Manager database.
- The vCenter Site Recovery Manager Server and the vCenter Server must be able to communicate over the network on all required ports.
- A vCenter Site Recovery Manager license is required to bring the server out of evaluation mode.
- The same vCenter Site Recovery Manager license should be installed on the vCenter Server instances at both sites.
- VMware Tools must be installed and updated in all protected virtual machines.
- Storage Replication Adapters (SRAs) must be configured if array-based replication is used.
- A non-replicated datastore is required at each recovery site to store placeholders for virtual machines.

**vSphere Replication Agent**

The vSphere Replication agent runs on each ESXi host that runs protected virtual machines. The vSphere Replication agent is a native component of an ESXi host and does not require additional installation or configuration.

The agent consists of two components:

- vSphere Replication service
- vSphere Replication filter

**The vSphere Replication Service**

- Schedules the creation and transfer of blocks modified by guest operating systems.
- Replicates the virtual machine’s metadata files (.vmx, .nvram, .vmxf).
- Stores a virtual machine’s replication configuration in the .vmx file.
- Coordinates group consistency for disks of a virtual machine.
The vSphere Replication Filter

- Attaches to the virtual device and intercepts all I/O to the virtual disk.
- Tracks changed blocks.
- Keeps the replication-specific state for individual disks.
- Transfers data to the vSphere Replication server.
- Implements logic necessary to guarantee data consistency.

Inventory Mappings

Inventory mappings provide a convenient way to specify how resources at the VMware vCenter Site Recovery Manager protected site are mapped to resources at the recovery site. These mappings are applied to all members of a protection group when the group is created (Sam Shouses Blog, 2014).

Resource Mappings

Resource mappings define which compute resources are used at the recovery site when virtual machines are recovered.

Folder Mappings

Folder hierarchies are used to help you organize which virtual machines are only local and which ones come from the protected site. These hierarchies also help you categorize virtual machines by their purpose, their recovery point and recovery time objectives, and other criteria.

High Availability and Disaster Recovery

High Availability has solutions to eliminate risks of a single-point failure by using secondary (redundant) sites or servers in the following ways:

- Real-time synchronization of data.
Providing a quick response to hardware failures or unplanned outages based on real-time replication.

- Redundant servers.
- Replication over a local network.
- Localized Solution: disk redundancy, server redundancy, network interface and path redundancies, and redundant server power supplies.

Disaster recovery is a method for backing all the files and applications efficiently and making them immediately accessible after an outage or failure. Such an outage or failure can be caused by a natural disaster, power outage, human error, or deliberate attacks on a datacenter. A disaster recovery plan contains procedures and processes to protect resources and ensure quick recovery from an outage.

A Disaster Recovery Solution can be implemented in a physical datacenter or a virtual datacenter using solutions like those from VMware. Implementing a DR in a physical datacenter presents distinct challenges:

- Requires identical hardware for recovery, which increases design complexity and cost.
- Requires significant amounts of time to orchestrate fail-over and fail-back in the case of an outage.
- Involves a slow and complex recovery process wherein different solutions will be used for different availability tiers and different storage types (Viltorius, 2015, VMware, n.d.f).
Advantages of Virtual Disaster Recovery

- Virtual machines are encapsulated into files, which are portable.
- Virtual machine hardware can be automatically configured.
- Failover and recovery plans can be easily tested.
- The requirement for identical hardware is virtually eliminated.
- Lower overall cost.

VMware High Availability

VMware vSphere High Availability is a feature which can protect virtual machines from unplanned downtime in the case of an ESXi server failure. HA is a cluster-level feature that allows up to 32 ESXi servers (vSphere 5.5) or 64 ESXi servers (vSphere 6) to be placed into a logical cluster. Once HA is enabled on a cluster under vCenter server, fault domain manager (FDM) agents are invoked on all cluster servers and an election process is held to choose a master node.

![Diagram of High Availability](image)

*Figure 8. High Availability (Listwon, n.d.)*

The master node will initially be chosen based on which one has the most connected datastores. In the case where there are two servers with same number of accessible datastores, vCenter will elect a master node based on the managed object ID (MOID), which is a unique
identifier assigned to each ESXi host when it is added to vCenter. Once a master node is elected, the master will start monitoring all the ESXi hosts in the cluster for a failure. If a slave is not responding to the master node with regular “heartbeats,” the slave is considered either dead or isolated. The master node then checks on the datastore heartbeat of the slave and takes an appropriate action on the virtual machines currently running on the failed node.

If a server is dead, the master will simply restart the failed server’s virtual machines on another host in the same cluster. If a slave is still online but isolated for some reason, then the master will check on the host isolation response configured on the cluster and take an appropriate action. The potential responses in the case of an isolated host include leaving the powered-on VMs on the isolated server or, as in the case of a failed host, restarting them on another host.
Chapter IV
IMPLEMENTATION

ESXi Installation

Installing ESXi on a physical server is a fairly straightforward process.

- Insert an ESXi 5.5 installation CD into the server’s optical drive. Change the boot order in the system BIOS so that it boots to the optical drive first.

- Wait 3-5 minutes for the installer to load.
- Accept the End User License Agreement.

- The installer scans for attached hardware and loads the necessary drivers.

- The installer next scans for available storage devices and volumes. Select a local installation destination and continue.

- Select the desired keyboard layout.
• Enter F11 to begin the installation.

• Once the installer has finished, press Enter to reboot the system.

• Press F2 and provide the root user credentials to start configuring the ESXi server.
• Select Configure Management Network and assign a static IP address to the server.

• Once the IP configuration is done, press “Y” to apply the changes and restart the management network.

Log on to ESXi

To connect to an ESXi server we can use any of the following methods:
(a) vSphere Client, (b) SSH client, (c) Shell or direct console on the server and (d) vCenter Server
vSphere Client, SSH, and vCenter are all remote connectivity tools which allow administrators from different geographies to manage an ESXi server. The ESXi server shell can be used only if an administrator is physically in front of the server. If Lockdown Mode is enabled on a server, all remote access attempts will be blocked and the server can only be administered from the console or a vCenter Server instance. This helps increase the security of the ESXi server.

Shell and SSH access can be enabled from the DCUI of an ESXi server. To enable the shell, simply navigate to troubleshooting options on the ESXi customization screen, select troubleshooting options, and select ESXi shell from the menu. Once the shell is enabled, pressing ALT-F1 at the console will allow an administrator to type commands at the ESXi command line. To return to the DCUI interface, press the ALT-F2 hotkey combination.

To connect to an ESXi server using SSH, log into ESXi using the root account, navigate to troubleshooting options on the ESXi customization screen, and select ESXi SSH. Connecting to an ESXi server via SSH requires that the administrator have an SSH client application, such as PuTTY.

vCenter Server

vCenter server is a centralized management platform that can manage multiple ESXi servers and the virtual machines running on them. Two types of vCenter servers are available and, while they provide nearly identical feature sets, each has its own advantages and limitations.
Table 1

*Significant Differences between Windows-based and Linux-based vCenter Deployments*

<table>
<thead>
<tr>
<th>Windows-Based vCenter Server</th>
<th>Linux-Based Virtual Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports IPv6</td>
<td>Does not support IPv6</td>
</tr>
<tr>
<td>Can be installed either on a physical server or on a Virtual machine. VMware recommends running vCenter in a virtual machine</td>
<td>Can only be installed inside a VM</td>
</tr>
<tr>
<td>Supports Microsoft SQL Server, Oracle and IBM DB2 as external databases</td>
<td>Supports Oracle as an external database</td>
</tr>
<tr>
<td>The embedded database is a SQL Express instance. This Embedded database supports only 5 hosts and 50 virtual machines</td>
<td>PostgreSQL is the embedded database. Version 5.5 supports 300 hosts and 1,000 virtual machines, while version 6 supports 1,000 hosts and 10,000 virtual machines</td>
</tr>
<tr>
<td>Supports VMware Update Manager</td>
<td>Does not support VMware Update Manager</td>
</tr>
<tr>
<td>Linked mode configuration is supported</td>
<td>Does not support linked mode configuration</td>
</tr>
<tr>
<td>Available as a separate application. Supported operating systems include Windows Server 2008, Server 2008 R2, Server 2012, and Server 2012 R2</td>
<td>Embedded SUSE Linux Enterprise Server 11</td>
</tr>
</tbody>
</table>

**vCenter Server Architecture**

Before installing a vCenter Server, FOR instance, we need to install three prerequisite components: (a) Single Sign On, (b) Web Client, and (c) Inventory Service.

*Figure 9. vCenter Server Architecture (VMware, n.d.)*
Single Sign On allows users to authenticate to vCenter and different modules with a single user name and password. To facilitate this, SSO depends on an existing Active directory, LDAP, or NIS infrastructure. Once SSO is installed, it creates its own internal domain (vSphere.local, by default).

Web Client can be used to connect to a vCenter Server instance in the same way as the traditional vSphere Client. However, the Web Client is the suggested method of administering vSphere infrastructures since version 5.5. In fact, there are new features added in versions 5.5 and 6.0 that are not available in the native vSphere Client.

The Inventory Service servers two primary roles: (a) It maintains the tags for Web Client, and (b) it acts as a proxy or cache for Web Client connections.

If users are connecting to a vCenter Server using the Web Client, all the connections will be cached by the Inventory Service. The next time the same users attempt to log into vCenter, the Inventory Service will look for and verify the connection details in the cache, thereby decreasing the load on the vCenter Server.

**vCenter Server Specification Requirement**

vCenter Server is a very critical component in the vSphere product suite. vCenter Server is a centralized management platform which can manage multiple ESXi servers. vCenter server can be installed on a supported Windows operating system or deployed as a Linux-based virtual appliance.

A single Windows-based vCenter Server instance can manage up to 1,000 ESXi servers and 10,000 powered-on virtual machines. vCenter Server requires a back-end database to store information about all of the ESXi servers it is managing.
Windows-based vCenter Server Requirements

Table 2

vCenter Server Requirements for Windows

<table>
<thead>
<tr>
<th>RAM</th>
<th>Four GB (minimum)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Four cores (minimum)</td>
</tr>
<tr>
<td>Hard disk</td>
<td>Seven GB free disk space (minimum)</td>
</tr>
<tr>
<td>Installation Mode</td>
<td>Can be installed on a physical server or on a virtual machine. VMware recommends installing vCenter Server on a VM</td>
</tr>
<tr>
<td>OS Requirements</td>
<td>Operating system should be assigned a static IP address, should be a part of an Active Directory domain, and should have VMware Tools installed (if running as a VM). The vCenter installation should be performed using a domain administrator account.</td>
</tr>
</tbody>
</table>

Linux-based vCenter Server Requirements

Table 3

vCenter Server Requirements for Linux

<table>
<thead>
<tr>
<th>RAM</th>
<th>Two GB (minimum)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Four cores (minimum)</td>
</tr>
<tr>
<td>Hard disk</td>
<td>Four GB (minimum)</td>
</tr>
<tr>
<td>Operating System</td>
<td>Comes as an OVA virtual appliance based on SUSE Linux</td>
</tr>
<tr>
<td>Installation Mode</td>
<td>Deployed into vCenter as a virtual appliance with pre-configured virtual hardware.</td>
</tr>
</tbody>
</table>
vCenter Server Installation

Installing vCenter Server as a Linux-based virtual appliance involves the following steps.

In order to deploy the VCSA virtual appliance, the OVA file must first be downloaded from VMware.

- Connect to an ESXi Server using vSphere Client. Click on File and select “Deploy OVF Template” from the menu.

- Locate and select the download OVA file. Click Next to continue.

- On the next stage of the wizard it shows the description of the product. It is vCenter Server Appliance version 5.5 running on SUSE Linux Enterprise Server 11.
- Name the vCenter virtual appliance and click Next to continue.

- Select the datastore where the appliance should be stored and click Next.
Select the provisioning type for the appliance’s virtual hard disk. Three types of virtual disk provisioning are available:

- **Thick Provision Lazy Zeroed**: In this provisioning type, all storage space will be allocated immediately. However, the formatting of the hard disk will happen as needed.

- **Thick Provision Eager Zeroed**: In this provisioning type, all storage space will be allocated up-front. The formatting of the hard disk will take place immediately as well. This is the best option for running business-critical applications, as the applications need not wait for the formatting to take place.

- **Thin Provision**: In this provisioning type, virtual disk space is allocated on-demand up to a user-defined maximum. The primary benefit of thin provisioning is that there will be no wasted disk space. However, because a VM with a thin-provisioned virtual disk must wait for disk space to be allocated, there is a small performance degradation.

Next, select the virtual network that the appliance should be connected to, and click Next to continue
• The deployment of the virtual appliance will begin.

• Once the deployment is complete, select the vCenter Server VM and power it on.

• Once the appliance finished booting, we next need to configure the management network interface, default gateway, and hostname of the appliance.
Next, log into the manage console of the appliance using the default password "vmware" and run the command /opt/vmware/share/vami/vami_config_net to begin the post-installation configuration.

The vami_config_net command brings up a menu through which we can configure several aspects of the vCenter appliance.
• Make any configuration changes necessary, and select option 2 to close the configuration menu.

We can now access the web-based administration console. Open a supported web browser and enter the hostname of the appliance in the address bar. Be sure to specify port 5480 at the end of the address.
- Accept the EULA and click Next to continue.

- Continue through the setup wizard, providing the appropriate information for the vCenter environment.

- Now we can log into the vCenter Server appliance using the traditional vSphere Client by specifying the IP address of the appliance.
SRM Database Setup Using Microsoft SQL Server 2008 R2 Express

Download SQL Server Management Studio (SSMS) installation files (SQLManagementStudio_x64_ENU.exe / SQLManagementStudio_x86_ENU.exe) from the SQL Server download page depending on your server type (x64, x86), and keep it in a separate folder.

Once you downloaded the respective file as per your server type, you need to execute it. It will then take you to the SQL Server Installation Center, this is the primary installation of SQL Server. Other SQL server tools installations can be launched from there as well. Once you are on that screen, you need to select “New SQL Server stand-alone installation or add features to an existing installation” to proceed with the installation.

After Downloading and Installing SQL Server Management Studio (SSMS), open it and create a new database by following these steps.

- Right-click on the Databases folder and select New Database from the menu.
Create a new database for System Resource Manager by completing the New Database wizard.

Create a new user for the database created in previous step by right-clicking on the Login option (under the Security node) and selecting New Login from the menu.
• Create a Login Name and Assign it a Password. Do not check the enforce Password Expiration Option as the Password has to be changed in 30 days.

• Select the Public option from the list of server roles.
• Next, map the user created in the previous step to the database by clicking on the user mapping, selecting the role membership as public and db_owner.

The next step involves creating a schema for SRM: Select databases, expand and select the new created database, click on Security, right-click on Schema, and select New Schema from the menu.
• Specify a name for the new schema and click OK to continue.

• Next, expand the Security folder under the database tree, right-click the new user account, and select Properties from the menu.
Now on default schema option select the name that we have created. For this deployment, we used “vmwaresrm” as the name for the database, user account, and schema.

Next, we have to make sure the database allows SQL Authentication. Right-click on the database and click on Properties from the menu. Navigate to Security Options and click on SQL
and Windows Authentication mode. Restart the SQL Server database services to ensure that the authentication changes take effect.

Next, we need to set up the 32-bit DSN for SRM so that SRM can connect to the database. Browse to C:\Windows\SysWOW64, select odbcad32.exe, and launch as shown in the following screenshot.

Navigate to the System DSN tab and click the Add button. In the new window, select SQL Server Native Client Version 10.0, and click Finish.
• Assign a name to the DSN and enter the correct and path for the server. For our deployment, we used the SQL Express embedded database included with the vCenter Server installation. The database name is VIM_SQLEXP.

• Select the radio button next to “With SQL Server authentication…” and specify the database login ID and password set earlier.
• Click on “Change the default database to:” and specify the name of the SRM database.

• Accept the defaults and click Finish.
• All configured options will be displayed. Review them for correctness and click OK to complete the ODBC connector setup wizard.

• Optionally, the DSN can be tested by clicking on the Test Data Source button. If everything was configured properly, the test should be successful as shown below.
Chapter V

SITE RECOVERY MANAGER

Site Recovery Manager

Site Recovery Manager, aka SRM, is a Disaster Recovery Solutions from VMware. It makes use of either vSphere Replication or Storage Array Based Replication to Recover Virtual Machines from a Disaster (VMware, n.d.b).

Key Benefits of Using SRM

- SRM greatly simplifies and automates test and failover operations.
- Works along with VMware vSphere to enable faster, simpler, and more cost-effective disaster recovery.
- Allows failover configuration to be set on a per-VM basis.
- Administrator can expand disaster recovery protection to any application with minimal effort and cost.
- Allows for single-click recovery of hundreds of virtual machines, drastically reducing the time required for recovery.
- Eliminates hardware dependencies, as all components necessary for failover are virtualized.
- Simplifies the failover testing process to help ensure better preparedness in the case of an actual failure/disaster.
- Recovery and failover plans can be designed and modified dynamically in response to changing environments.
- Reduces capital and operating expenditures.
**Installation of Site Recovery Manager (SRM)**

The installation media for Site Recovery Manager can be downloaded from the VMware website. To be able to download software from VMware, the user must first register for a VMware account and request a trial version of the product. We used the trial version in this paper.

Once the download is completed, start the installation on a machine which is running vCenter server or on a separate virtual machine running a supported Windows operating system. The installation of SRM should be carried out both in the protected and recovery sites.

- To begin the installation, mount the installation media and launch the included installer.

- Once the wizard starts, click Next and agree to the license agreement.

- Specify an installation location and click Next to continue.
• Specify the vCenter Server Platform Services Controller address and port. The address must be a full-qualified host name or address. Also, specify the credentials of a Single Sign On account with administrative privileges, and click Next.

• Select the vCenter Server instance for pairing up the SRM, and click Next to continue.
- On the next stage of the wizard, specify a name for the site and an email address, and select the IP address of the host where SRM is installed.

- Let the wizard generate a SSL certificate. The certificate will be used to secure SRM traffic between servers.

- SRM server requires a database, which can be either a dedicated SQL Server database or the integrated database that comes bundled with SRM. It is recommended to have a separate, dedicated database in real production environments.
• Specify the DSN, database username and password, and port number for the database connection. The port will be 5678 by default, and it is recommended to not change it unless this port is being used by some other service. Finally, specify the database connection count and maximum connections limit, and click Next to continue.

• Provide credentials for either a local system account or domain account under which the SRM service will be run.
- Once all steps of the wizard are complete, click Install to begin the SRM installation.

- Click Finish to complete the installation.
Log into the vCenter Server in the primary/protected site using the vSphere Web Client and verify that Site Recovery is shown.

Repeat the same steps to install SRM at the secondary/recovery site. Once the installation is complete in the secondary site as well, log into the vCenter Server at the secondary site and verify that Site Recovery is present there as well.

**Array-based Replication**

Array-based Replication for business continuity can incorporate the creation of local copies of data within the same array as the source data, as well as the creation of remote copies in an array located elsewhere. Many enterprise storage vendors offer sophisticated technologies
that provide this functionality, driven either from the arrays themselves -- via management hosts that control the direction and identity of replication -- or within a virtualization layer that operates in the SAN fabric or IP storage network.

Creating local and remote replicas of data gives an organization a limited form of business continuity and enhances its operational readiness by creating data copies that can be used for testing and development. Using storage technology, this is achieved at the volume level with features such as Quality of Service (QoS), priority controls, data consistency, source-target identity swaps, duplex data flow, protected copies, data queuing/batching, and full or pointer-based read/write.

The same functionality can be approximated at the host layer by using Logical Volume Manager (LVM) and plexes/mirrors as well as any "snap" functionality that may exist in the host LVM software. However, the feature set tends to be limited and management more painstaking due to the need to operate within LVM and in close logical proximity to the source data.

Creating local replicas for the purpose of business continuity is easily achieved using LVM when only one to three copies of that data are required. However, when four or more copies are required, and the business demands time-specific restore points, it is advisable to create replicas using the storage software. This is because there is a greater ability to create a large number of copies that can be synchronized and detached at specific intervals using advanced algorithms for incremental and full-data copy. This, combined with intelligent space management techniques such as copy on read/write, make the storage software offering highly effective.
Installing HP SRA for SRM

For this research paper, we used an HP StoreVirtual (SV) storage appliance for VM storage. This provides array storage functionality for vSphere without requiring an external storage box. It makes a server’s internal storage available to ESXi servers as shared storage volumes. To download HP SV, registration is required on the HP website: https://www.hpe.com/us/en/storage/storevirtual.html.

Once HP SV is downloaded, the centralized management software should be downloaded as well. This additional software component is used to create storage LUNs and configure replication capabilities.

The steps required to install and configure HP SV are outlined below:

- Launch the downloaded installer and extract the files to a convenient location. Double-click Virtual_SAN_Appliance_launcher.exe and select option 2 to launch the graphical installation wizard.

- A welcome message is displayed. Click Next to continue.
- Accept the license agreement and click Next to continue.

- Deselect the Skip CMC (Centralized Management Console) Installation option and click Next.

- Provide the IP address and root user credentials for the ESXi where the appliance should be deployed.
- Review the ESXi host and datastore information, and click Next to proceed.

- Select HP StoreVirtual VSA as the installation type. Additional options like Space Reclamation and multi-tiered storage support can be selected. Click Next to continue.
• Select the datastore to deploy the HP SV appliance to, and click Next.

• Assign an IP address, DNS name and virtual machine port group to the appliance. Click Next to continue.
• Specify a name for the virtual appliance, and select VMDK as the drive type. Click Next to continue.

• Select a location for VMDK files on the ESXi server. This will be the storage destination presented to ESXi hosts as a datastore. Click Next to continue.
- If desired, a second virtual appliance can be deployed with the same wizard. Click on No, I am done click Next to continue with just the one SV appliance.

- A progress screen will be displayed as the deployment proceeds. Once complete, click Finish.
Repeat the same steps to deploy the HP SV appliance at the secondary site, which can be used to map datastores to the ESXi servers in the secondary site. Once this process is complete, SRM uses those datastores for array-based replication.

**Configuring HP Virtual Storage Array.**

Once our virtual storage appliances have been deployed, we need to perform some configuration steps to make the appliance’s storage resources available to the VMware infrastructure. Log into the vCenter Server instance at the protected site and complete the following steps.

- Locate and launch the HP SV Centralized Management Console installer. Specify a language preference and click OK to continue.

- On the Introduction screen, click Next to continue.
• Select the Typical install set, and click Next to continue.

• The rest of the installation steps should not require any specific user input. Click Next as necessary to complete the wizard.

• Once the installation is complete, launch the HP CMC application. It should detect the HP SV appliance(s) that were deployed on the ESXi servers automatically. If the auto-detection fails, we can locate the HP SV appliance manually by clicking on the Find button.
• Click on Login to view on the HP SV appliance that was deployed in the previous steps to review the storage appliance configuration.

• After log in

• Next, we need to create a management group. Right-click the VSA node and select Add to New Management Group from the context menu. Create two management groups, one for the primary site and the other for the secondary site. These groups will be used by SRM for array-based replication.
- Specify a name for the management group and click on Next to continue.

- Create an administrative user to manage the group. Click Next to continue.
• Configure the time setting using a Network Time Protocol server, assign a DNS server, and select the cluster type as shown below. As one VSA is being used per site, select Standard Cluster.

• Provide a name for the cluster and add the first VSA.

• Assign an IP address and subnet mask to the cluster. This IP will be used as a storage target for the ESXi servers when adding a datastore.

• We are now able to create a volume and provision space to it.
- Repeat the same steps to create a management group and provision storage for the secondary site.

Add the ESXi Server to the HP CMC. We can now see the datastores presented to the ESXi servers. Right-click on the Servers node and click on New Server from the context menu.

In the New Server dialog, we can configure details about the server that will be accessing the VSA storage. Provide a name and IP address for the vCenter Server instance. Specify an iSCSI IQN address, configure load balancing (if desired), and configure CHAP authentication for connections to the VSA.
Follow the same steps to add the server in the secondary site as well.

As the ESXi hosts are already added to the management group, the next step is to make the ESXi servers access the storage volumes created in the earlier steps. To perform this operation, right-click on the storage volume and click on Assign and Unassigned Servers from the context menu.
• Locate the primary site ESXi server from the list and select the Assigned checkbox.

Next, log into the ESXi server, click on Configuration, click on Storage Adapters under Hardware, click on click of the adapter and click on dynamic discovery and add the virtual IP of the management cluster created in the previous steps. Click OK.

Finally, complete the same steps for the secondary site.

**Pairing Site Recovery Manager Servers**

Once the HP SV appliance installation is complete and the SRM plugin appears in the vCenter Servers at both sites, we next need to pair the two sites so they can be used as a single DR group. Using the vSphere Web Client, log into the vCenter instance at the protected site,
click on Site Recovery, and click on Sites as shown below. Complete the following steps to pair the two sites.

- On Sites, click on the Summary tab and then click on the Pair Sites option.

- Specify the IP address or fully-qualified domain name of the Platform Services Controller at the secondary site. Leave the port number at the default setting. Click Next to continue.

- Once the PSC is specified, the wizard detects the vCenter Server associated with the PSC. Enter the Single Sign On credentials of the vCenter Server.
Once the pairing is complete, the wizard will automatically show the primary site and secondary site information as shown below.

The configuration can also be verified by connecting to the vCenter Server instance at the secondary site. This pairing process need only be completed at one site, and will be reflected at both.
Once the two sites are paired, we next need to configure the HP Array Manager at both sites.

**HP SRA Array Manager for SRM.**

The HP Array Configuration Utility (ACU) provides online, high availability configuration, management, and diagnostic capabilities in support of all Smart Array products and particular HP ProLiant Storage RAID Array Controllers. The software consistency of the related tools reduces the cost of training for each successive generation of product and takes much of the guesswork out of troubleshooting field problems. These tools lower the total cost of ownership by reducing training and technical expertise necessary to install and maintain HP server storage.

HP Array Configuration Utility 64-bit is a program developed by Hewlett-Packard. The software installer includes seven files and is usually about 5.55 MB (5,816,320 bytes). In comparison to the total number of users, most PCs are running the OS Windows 7 (SP1) as well as Windows 8 (Hewlett Packard, 2015).
Configuring the HP Array Manager at the primary and secondary sites.

- Click on Rescan All. After a short wait, the storage LUNs provided by the VSA will be detected. Add the LUN as storage to the ESXi host.

- Repeat the same steps to add the LUN to the ESXi at the secondary site as well.

Now that the primary and secondary sites are paired and have access to shared storage, we can configure replication between them. Storage replication allows the VMs on the shared storage volumes to replicate to the secondary site if something should happen to the primary site. To configure this, right-click on a volume at primary site and click on New Schedule to Remote Snapshot a Volume option, and proceed with the following steps.
Assign a name to the replication schedule and add the secondary site management group and the volume of the secondary site under remote snapshot step. The retention time for the snapshot option can be selected, if required. Click OK to continue.

- Storage replication is now enabled between the primary and secondary sites.

VMware SRM has the capability to replicate data from a primary site to a DR site using array-based replication. For this to function, a Storage Replication Adapter (SRA) must be installed in both the primary and disaster sites so that the array manager on the SRM can do array-based replication. The steps to configure replication between sites are given below.
• Log into the server running the SRM instance at the protected site and download the SRA installer from the VMware website. Launch the installer to continue.

• Accept the license and click Next.

• Click on Install to begin the SRA installation.
Once the installation is complete, click Finish.

The SRA installation will automatically be detected by the SRM server and can be seen within the vSphere Web Client as shown below.

Repeat the same steps to install the SRA at the second site.
Next, we need to add the array manger on the Web Client. Click on SRM within the Web Client session, select the primary site, click array-based replication, and click on the icon shown below.

- Select the Add a pair of array mangers option to configure the array at both sites.

- Select the pair of sites, and click Next to continue.

- The SRA will be automatically detected. Click Next to continue.
• Provide a name for the new array, provide the credentials for the primary array manager, and click Next to continue.

• Provide the corresponding information for the secondary site as well.

• Select the array pair and click Next to continue.
• Review the array configuration and click Finish.

• Within the vSphere Web Client, click on Array Based Replication and navigate to the Objects tab. Confirm that an “OK” status is shown for both array managers.

• Select one of the VSA in the left-hand pane. Replicated datastore information will be shown for the VSA pair.
The next step involves configuring the inventory mapping between vCenter Servers at both sites. This will ensure that mappings exist between the clusters and resource pools at the primary and secondary sites, which is required by SRM to recover the virtual machines based on preferences set by the administrator. Once the mappings have been established, SRM will execute the recovery plan in the case of a disaster event, and the virtual machines will be restarted on the vSphere resources at the other site.

**SRM Resource Mappings**

- To create the necessary resource mappings, log into vCenter using the Web Client, click on SRM, select the protected site, and then click on Create resource mappings.

- Select the primary site, select the ESXi server at that site, select the newly-created mapping resources, and click on Add mappings.
- Configure the mappings as per the folder structure required as shown below.

- Select the objects for reverse mapping. This will create the reverse mappings automatically on the paired site. This is required to do a failover from the secondary site back to the primary site. Click on Select all applicable and click Finish.

- To verify the resource mappings, click on the Manage tab on the primary site and navigate to the resource mappings tab as shown below.
SRM Folder Mappings

Once the necessary resource mappings have been configured, we need to map any organizational folders between the sites as well. This ensures that virtual resource organization is consistent between the two sites. The folder mapping procedure is described below.

- Click on SRM, select the primary site, and click on the Create folder mappings option under inventory, as shown below.

- These folder mappings can be done automatically and manually, select manual and click next.
• Select the folders in the primary site and the corresponding folders on the recovery site and click on Add mappings to the create folder mappings.

• Select the folder mapping on the primary and secondary sites as shown below. Click Next to continue.

• Select all the required reverse mappings and this will automatically create the mappings between the paired sites. Click Finish.
Once this process is complete, the configuration can be verified by clicking on the Manage tab on the site and navigating to folder mappings as shown below.

Next step involves the network mapping on the primary site to secondary site. This is required for the virtual machines powered on the disaster site should get connected to the network after a recovery plan is successfully executed by SRM. Select the virtual machine port groups on the primary site and map them with the port groups on the secondary site.

**SRM Network Mappings**

- Click on the SRM on the protected site by logging on to the vCenter Server. Click on summary tab and click on Create Network Mapping Option.
• Just like folder mappings again, the same options are available. This network mapping can be done automatically or manually, click on manual and click next.

• Select the virtual machine port groups on the primary site and map them with the port groups on the secondary site and then click on add mappings. Virtual machine port groups are where virtual machines get connected and can talk to each other.
• Repeat the same and click next between the paired sites for different networks.

• Once all the networks are mapped click on finish.

• The same can be verified by clicking on the SRM, click on primary site, click on manage, click on network mappings options.

Next step involves creating a placeholder Datastore which will be used to place the virtual machines in the recovery site. It reserves the place for VM in recovery site inventory. These Datastores are to be seen by all severs in the cluster. These are to be created on both sites to enable failover to both sites. Place holder VM is a set of VM files that are created. Any VM
added to recovery plan cannot be powered on. As soon as a VM is added to protection group, a placeholder VM will be created in the recovery site.

SRM Placeholder Datastores

- To create a placeholder Datastore, click on configure placeholder Datastore under SRM.

- Net step involves selecting a Datastore to be used as a placeholder for the production virtual machines. Replicated LUN cannot be used for placeholder Datastore. Click OK

- Placeholder is configured and can be seen under manage, click on Placeholder Datastores.
• Repeat the same steps on the secondary site as well. This has to be a non-replicated Datastore on the secondary site again. Click OK

SRM Protection Group Creation

Next step involves creating a protection group, which is also a place to put the VM’s that are to be protected by SRM. To create a protection group, click on create protection group under summary of SRM screen. Give a name and select the site.
• Select the primary site, the type of replication for the protected group created. Both vSphere replication and array based replication cannot be selected together, click next.

• Select the Datastores from the list to create a Datastore group. All the VMs on the Datastores will be recovered as part of the protection group. Click next.

• Re-check and click Finish.
Next step is to create a recover plan. Recovery plan is an automated plan for to recover the protected VMs in the recovery site should a disaster happen in the datacenter. A group of virtual machines can be included in multiple recovery plans. A recovery plan includes the list of virtual machines from all the protection groups in it. It also includes the startup priority of virtual machines should a disaster happen and also a customization to be followed after the virtual machine starts from recovery.

The customization includes IP for VMs after recovering, login scripts. Virtual machines which are recovered can be placed in to isolated network in order to make sure the production machines will not get effected.

**SRM Recovery Plans**

- To start creating a recovery plan, click on SRM, click on summary and then click on create a recovery plan, click ok
• Select the site on to which virtual machines are to be restarted should a disaster occur, click next.

• Select the protection groups, which are included in the recovery plan. Click next.

Click on Next. Test networks can be specified on the recovery site if the admin wants the recovered virtual machines to be connected to the test network after a recovery in order to let the production virtual machine run without any disturbance, or the admin can make use of the automatically created test network for placing the recovered virtual machines. Click next.

• Re-check all the settings specified and click finish.
Recovery plan created can be seen under the sites option on the web client. The recovery plan can be edited to change the VM priority and the networks.

SRM Testing and Failback

Next step involves testing the recovery plan created. SRM ensures that a disruptive testing can be done without affecting the virtual machines which are already running on the server in both the sites.
To test a recovery plan, click on recovery plans options, then click on monitor tab, the click on recovery steps and then click on the play button as shown in the below screenshot.

Once the play button is clicked on, the recovery will run in test mode without affecting the virtual machines already running on the servers on both the sites. Select the option replicate recent changes to the recovery site so as to get them replicated. Click next.

Re-check the settings and click finish.

Once test is being executed a series of steps can be seen on the recovery steps option.
• The status of the recovery plan can be seen once it is completed.

• Once the test is completed, the virtual machines the virtual machines can be seen running on both the sites.

• Clean up process is as important as creating a recovery plan. This can be done by click on the recovery plan, click on the brush symbol as shown below.
- By click on the cleanup option the test environment will be removed completely and the sites will be back to normal functioning state.

- Re-Check and click on finish to start the cleanup.

- Monitor the task and making sure that all the VM are up and running.

- It will now get everything back to a previous known state.
The virtual machines are now in a powered off state after the cleanup operation. We can now create another recovery plan if required and that also can be tested multiple times without affecting the running state of the virtual machines on both sites.
Chapter VI

TIMELINE

Table 4

Dates and Description of the Task

<table>
<thead>
<tr>
<th>Start Date</th>
<th>End Date</th>
<th>Task(s)</th>
<th>Duration (Days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/16/2015</td>
<td>4/29/2015</td>
<td>Winding up the Data Collection</td>
<td>14</td>
</tr>
<tr>
<td>5/1/2015</td>
<td>5/7/2015</td>
<td>Acquiring Physical Servers</td>
<td>7</td>
</tr>
<tr>
<td>5/9/2015</td>
<td>5/20/2015</td>
<td>Required software’s and OS licenses.</td>
<td>12</td>
</tr>
<tr>
<td>5/25/2015</td>
<td>6/15/2015</td>
<td>Installation and Configuration of Physicals Servers</td>
<td>11</td>
</tr>
<tr>
<td>6/20/2015</td>
<td>7/09/2015</td>
<td>All VMware and Necessary features will be installed</td>
<td>20</td>
</tr>
<tr>
<td>8/1/2015</td>
<td>8/10/2015</td>
<td>Implementing the replication.</td>
<td>10</td>
</tr>
<tr>
<td>8/11/2015</td>
<td>8/20/2015</td>
<td>Testing SRM</td>
<td>10</td>
</tr>
<tr>
<td>8/21/2015</td>
<td>9/15/2015</td>
<td>Complete report will be written on findings</td>
<td>25</td>
</tr>
<tr>
<td>9/16/2015</td>
<td>11/19/2015</td>
<td>Will be ready for final defense</td>
<td>45</td>
</tr>
</tbody>
</table>

I have met the estimated timeline as planned, though I have faced a few hurdles, it was all part of it.
Chapter VII

CONCLUSION AND FUTURE SCOPE

For Business Continuity and Disaster Recovery in a vSphere infrastructure, most customers make a choice of two options. Either use VMware Site Recovery Manager (SRM) or build a vSphere Metro Stretched Cluster.

Two datacenters in active/passive—one running production and the other test/dev. If production site fails, VMware Site Recovery Manager is used to perform an Orchestrated Recovery of the Virtual Machines in the recovery site. Tools used are vSphere Replication and Array Based Replication. This method is called as Disaster Recovery.

However, there is another method which is called as Disaster Avoidance—two datacenters, both running production in an active-active configuration with stretched storage and networking. We call this a vSphere Metro Stretched Cluster.

vSphere Metro Stretched Cluster is great for disaster avoidance, balancing of resources and planned maintenance. When IT knows in advance one of the datacenters might become unavailable because of a hurricane/downtime of power/SAN maintenance etc., virtual machines can be vMotion-ed to the alternate datacenter.

In case of an unplanned event like a fire or earthquake, VMware HA will take care of the restarts of virtual machine but the limitation is vMotion works well only in a round trip of 100ms. The advantage is that up-to-date virtual machine disk files are available in the recovery site so RPO as well as RTO is low.

However, VMware HA is not designed for large scale recovery of a complete site. VMware HA does not offer recovery plans for an automated recovery. It is not aware of
application dependencies nor is it site aware. HA does not offer a granular control over VM start priority. Also a failover cannot be tested. So we cannot shutdown and reboot a VM without taking a production VM down.

Another restriction is that because of the synchronous replication of the storage layer, the distance between the two datacenters is limited to about 100km. A vSphere Metro Stretched Cluster is typically deployed in a metro area.

So, in the future, we may expect vSphere SRM will be improved to smoothly integrate with vSphere Metro Stretched Clusters.
References


