One Touch Disaster Recovery Solution for Continuity of Operations

Rajat Ravinder Varuni
One Touch
Disaster Recovery Solution
for Continuity of Operations

Author: Rajat Ravinder Varuni CEH, CCSP, MCSE, CIWSP

Advisor: Stephen Northcutt, President
The SANS Technology Institute (www.sans.edu)
# TABLE OF CONTENTS

Abstract ..................................................................................................................... 4  
Introduction............................................................................................................... 4  
Objectives.................................................................................................................. 5  
Thesis......................................................................................................................... 5  
  A. Capacity Planning................................................................................................. 9  
  B. Network Configuration....................................................................................... 13  
  C. Storage................................................................................................................ 15  
  D. Global Traffic Managers.................................................................................... 16  
  E. The P2V process.................................................................................................. 19  
  F. VMware Site Recovery Manager (SRM)............................................................ 19  
    I. Pre-installation steps.......................................................................................... 20  
    II. Install SRM ...................................................................................................... 21  
    III. Post installation ............................................................................................. 25  
    IV. Testing the recovery plan from the DR site...................................................... 27  
    V. Configure for failback to primary data center.................................................. 28  
    VI. Testing the failback from the DR site............................................................. 28  
Project Timeline....................................................................................................... 28  
Concluding Remarks................................................................................................. 30  
Glossary of Acronyms............................................................................................... 31  
Bibliography............................................................................................................. 32
Abstract

In today’s digital age information is knowledge and knowledge is power. These days information is stored in computer systems across the world for ease of access and retrieval. However computer systems are subject to malfunction due to human error, floods, fire, acts of terror etc. In this publication I present a solution where information (while preserving its integrity) is available during or following a disaster. I call this, One Touch Disaster Recovery [DR] solution for Continuity of Operations [COOP].

For this solution I am leveraging the power of virtualization and global traffic managers. By doing so organizations will have a scalable environment which will facilitate easy deployment of applications, prevent server proliferation, comply with various Federal Computer Acts and Standards such as Healthcare Information Portability and Accountability Act of 1996, [HIPAA] and SAS 70 respectively, which would not only reduce the time for management of an application but also allow computer personnel to focus on further research & development. This would encourage innovation and in turn boost productivity. Thus increasing return on investment.

Introduction

For the purposes of this publication I have created a fictitious business to follow along. Let us call our business Aplils Medical Group [AMG] Inc.

AMG is proud to be the largest mental health association serving the most vulnerable citizens in the nation's capital. Since its founding in 1947, AMG has provided quality mental health care and residential services. AMG currently has six locations spread across the DC Metro area serving more than 23000 patients.

AMG’s staff accesses the medical records of their patients as needed from their workstations. AMG also has a clinic which provides round the clock health care services. The speed, accuracy and availability of the patients’ records are very critical to AMG’s business. Their Information Technology department has been tasked to design and implement a Disaster Recovery and Business Continuity Plan in compliance with the HIPAA.
**Objectives**

AMG has one primary data center and one disaster recovery [DR] site. AMG has an existing Active Directory Domain consisting of file, print, exchange, database, application and terminal physical servers. Currently all the critical servers are housed in the primary data center. The goal is to design and implement a disaster recovery plan such that AMG’s staff can have access to their patients’ medical records as needed during or following a computer disaster.

**Thesis**

Up until a few years ago, the traditional way of deploying applications on servers involved the following

I. Understand the applications’ hardware specifications.
II. Procure the server.
III. Install the server in the rack which also involves cabling
IV. Run diagnostics on the server’s hardware to detect any potential hardware issues.
V. Install the preferred Operating System.
VI. Update the hardware drivers and the Operating system
VII. Make sure that the cooling in the server room is sufficient
VIII. Install the application.

The above steps can be described as tedious at best, not to mention the time it took to remediate an unstable server. Deploying a set of servers with standardized settings was a hassle which required great documentation skills.

But now with the power of virtualization, multiple Operating Systems can be deployed within minutes, if not seconds. They can be concurrently run on a physical computer. The number of CPUs and the amount of memory can be changed on the fly without powering off the server. All of these functions and more can be achieved through a centralized management console which can be accessed remotely.

In short, deploying a server with standardized settings is just a click away!

Virtualization facilitates easy deployment of applications, prevents server proliferation by consolidating servers, hence eliminates the need for ongoing data center expansion.
Here is a chart which compares Virtualization products from VMware, Microsoft and Citrix.

<table>
<thead>
<tr>
<th>Most Efficient</th>
<th>VMware</th>
<th>Microsoft</th>
<th>Citrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Scale Out</td>
<td>64 logical cores, 512GB RAM</td>
<td>24 logical cores, 1TB TMM</td>
<td>32 logical cores, 12GB RAM</td>
</tr>
<tr>
<td>CPU Efficiency</td>
<td>CPUs are 8-way vCPU</td>
<td>Requires HW-assist for Win Reuse gen-OS scheduler</td>
<td>Requires HW-assist for Win Reuse gen-OS scheduler</td>
</tr>
<tr>
<td>Memory Efficiency</td>
<td>Memory HW-assist, Overcommitting sharing</td>
<td>Memory HW-assist, No overcommitment</td>
<td>Memory HW-assist, No overcommitment</td>
</tr>
<tr>
<td>Virtual Hardware (VM) Scale Out</td>
<td>256GB VRAM</td>
<td>4-way on Win 8 only, 64GB VRAM</td>
<td>8-way vCPU, 128GB VRAM</td>
</tr>
<tr>
<td>Hot-add/remove Virtual Resources</td>
<td>Add vCPU, vMem, Add virtual disk</td>
<td>None</td>
<td>No hot-add CPU, mem, Add virtual disk</td>
</tr>
<tr>
<td>Power Efficiency</td>
<td>DPM: Cluster-level power management</td>
<td>No Cluster-level management</td>
<td>No Cluster-level management</td>
</tr>
<tr>
<td>Storage Usage Efficiency</td>
<td>Thin provisioning monitoring tools</td>
<td>Thin disks, but no monitoring tools</td>
<td>Only by way of third-party storage vendor</td>
</tr>
<tr>
<td>Network Management Efficiency</td>
<td>Distributed switch, Third-party virtual switch</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Automated Patching Efficiency</td>
<td>Transparent host patch, Auto guest patching</td>
<td>Host patching causes VM downtime</td>
<td>Host patching but no auto guest patching</td>
</tr>
</tbody>
</table>

**Figure 1**
# Uncompromised Control

<table>
<thead>
<tr>
<th>Feature</th>
<th>VMware</th>
<th>Microsoft</th>
<th>Citrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control for Server Maintenance</td>
<td>VMware vMotion (w/ Enhanced Compatibility)</td>
<td>Quick Migration causes downtime</td>
<td>XenMotion</td>
</tr>
<tr>
<td>Control for Storage Maintenance</td>
<td>VMware Enhanced Storage VMotion</td>
<td>Nothing comparable</td>
<td>Nothing comparable</td>
</tr>
<tr>
<td>Control for Resource Allocation</td>
<td>VMware DRS Logical Resource Pool</td>
<td>Pro Tips has downtime No logical pools</td>
<td>Third-party for DRS No logical pools</td>
</tr>
<tr>
<td>Fault Tolerance for VMs</td>
<td>VMware Fault Tolerance</td>
<td>No VM-level protection</td>
<td>Promised feature hasn’t shipped yet</td>
</tr>
<tr>
<td>Control during NIC Failure</td>
<td>Integrated NIC training</td>
<td>Relies on network vendor to provide</td>
<td>Supported but may require CLI to configure</td>
</tr>
<tr>
<td>Control during Host or VM Failure</td>
<td>VMware HA Up to 32 nodes</td>
<td>Only for host failure 1-VM-per-LUN issue</td>
<td>Only for host failure Up to 18 nodes</td>
</tr>
<tr>
<td>Control during Entire Site Failure</td>
<td>VMware siteRecovery Manager</td>
<td>Geo-clustering has no workflow, testing audit</td>
<td>Nothing comparable</td>
</tr>
<tr>
<td>Thin Hypervisor to Reduce Attack Surface</td>
<td>VMware ESXi 70-100MB disk footprint</td>
<td>Hyper-V w/ Server Core &gt;2 GB disk footprint</td>
<td>XenServer 1.8GB disk footprint</td>
</tr>
<tr>
<td>Better Security than Physical</td>
<td>VMware VMAPI Third party support</td>
<td>Nothing comparable</td>
<td>Nothing comparable</td>
</tr>
</tbody>
</table>

# Maximum Choice

<table>
<thead>
<tr>
<th>Feature</th>
<th>VMware</th>
<th>Microsoft</th>
<th>Citrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choice through Guest OS Support</td>
<td>&gt;30 OSs supported More Windows than M5</td>
<td>11 OSs supported Windows biased</td>
<td>20 OSs supported</td>
</tr>
<tr>
<td>Choice through Hardware Support</td>
<td>Large HCL &gt;450 HBAs &gt;160 NICs, &gt;450 Servers</td>
<td>Using Windows drivers Potential driver issues</td>
<td>Very limited HCL ~100 Servers</td>
</tr>
<tr>
<td>Choice through Application Support</td>
<td>Leader category (according to a lead analyst firm)</td>
<td>Leader category(according to a lead analyst firm)</td>
<td>Next-tier category (according to a lead analyst firm)</td>
</tr>
<tr>
<td>Integrating with Existing Management Tools</td>
<td>Dozens of integrations vCenter API By SDK</td>
<td>Can integrate, but SC competes w/ existing</td>
<td>Citrix Essentials API not readily available</td>
</tr>
<tr>
<td>Choice in 'Cloud' Service Provider</td>
<td>VM Ready program for cloud providers</td>
<td>Building a MS-hosted offering</td>
<td>No dear cloud strategy</td>
</tr>
<tr>
<td>Interoperability between Internal &amp; External Cloud</td>
<td>VM Ready ensures interoperability</td>
<td>Apps in MS cloud don’t come back out</td>
<td>No dear cloud strategy</td>
</tr>
<tr>
<td>Choice in Using Existing Applications in the Cloud</td>
<td>Run existing apps w/o rewriting code</td>
<td>Apps need to be rewritten for MS cloud</td>
<td>No dear cloud strategy</td>
</tr>
</tbody>
</table>

This chart is up-to-date as of April 22nd, 2009.

It is clear that using VMware virtualization suite called vSphere will have an advantage over the rest. Most importantly VMware has features such as High Availability and Fault Tolerance which can protect our workloads with an uptime of nearly 100%.

**VMware vSphere High Availability**

In an event that a vSphere host becomes unstable due to hardware failure, software misconfiguration or power outage, the protected Operating systems running on the failed host are automatically migrated to stable vSphere hosts and rebooted.

![VMware vSphere Diagram](image-url)

**Figure 2**

**VMware vSphere Fault Tolerance**

Fault tolerance provides continuous protection for our Virtual Machines [VM] by running an identical VM on a separate vSphere server. At any event if the Virtual Machine on the current host stops responding, the corresponding clone takes over the operations without any delay, hence serving nearly 100% uptime.
Capacity Planning

Let us start by planning to virtualize our physical servers. The first and the foremost important step is to run the VMware Capacity planner, which not only gets current hardware inventory of our servers but also analyses the performance of the server hardware by collecting statistics during peak and off peak hours. The statistics collected which are mainly CPU, memory, network and disk utilizations help us plan for server, storage and networking hardware needed for virtualization in terms of capacity, performance and management. Ideally we would run VMware Capacity Planner for 30 to 60 days to determine if there is any anomalous activity.

“Develop a capacity plan before you need it, not when you need it.”

- Anonymous at VMWorld 2008

Next we need to decide which edition of VMware vSphere is best for the organization. To compare a list of features available between the vSphere4 editions visit http://www.vmware.com/products/vsphere/buy/editions_comparation.html

The vSphere Enterprise plus edition licenses features such as storage VMotion, Distributed resource scheduling [DRS], vNetwork Distributed Switch and host profiles.
Storage VMotion is a feature which enables live migration of Virtual Machine disk files between different storage arrays or shared datastores, while maintaining the integrity of the virtual machines operations, with zero downtime. Hence these migrations are non-disruptive for continuity of business operations. The following figure shows a graphical representation of vSphere Storage VMotion.

![VMware vSphere Storage VMotion](image)

**Figure 4**

Distributed Resource Scheduler [DRS] monitors the consumption of hardware resources by virtual machines such as disk, CPU and memory. If at any time the virtual machine needs more resources than available on the vSphere host, that virtual machine is migrated over seamlessly to another vSphere host server which has the necessary resources, all while the virtual machine is up and running. In other words, DRS does automatic load balancing of virtual machines between available host vSphere hosts. DRS can be configured such that the operations are fully
automated, hence do not need manual intervention and thereby freeing up time of VMware administrator. The following figure shows a graphical representation of vSphere Distributed Resource Scheduler.

**vNetwork Distributed Switch** provides administrators a centralized interface to configure networking for all virtual machines in each datacenter. As virtual machines migrate from one physical host to another, their network traffic needs to be monitored and secured. vNetwork Distributed Switch does this by maintaining a real time network state of each virtual machine. Additionally we can configure private VLANs and bi-directional traffic shaping for any virtual machine in the entire data center through a centralized interface. Therefore we get a consistent network configuration which is also scalable for future growth. The following figure shows a graphical representation of vNetwork Distributed Switch.
Host Profiles

In a data center consisting of several vSphere hosts, configuration of storage, networking and security settings could be tedious and often prone to error. By using a feature in vSphere called Host Profiles, we can standardize settings across all vSphere servers by deploying any changes in settings to all the vSphere servers securely.

Host profiles can also be used to monitor and report any compliance issues within the vSphere farm.

Since features such as storage vMotion, Distributed Resource Scheduler [DRS], vNetwork Distributed Switch and host profiles are highly useful for the primary data center and DR site, we choose VMware vSphere Enterprise Plus edition.

Figure 6
**Network Configuration**

Our vSphere farm has the following types of network traffic. They are as follows:

I. Service Console [vConsole] is used to configure and manage Virtual Machines.

II. VMKernel VMotion features such as VMHA, DRS need their own separate network.

III. VM production this is a dedicated network for production traffic.

IV. DMZ front end servers for exchange, Citrix and web servers shall be in the DMZ network.

To configure network redundancy and load balancing, we need two physical NICs teamed for each of the above four types of network traffic.

For each vSphere server we need a minimum of nine NICs. Here is a table describing their function. Refer to below network diagram for a detailed network diagram.

<table>
<thead>
<tr>
<th>Physical NIC #</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>vConsole</td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Vmotion, HA, DRS</td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Virtual Machine Traffic</td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>DMZ traffic</td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>DRAC</td>
</tr>
</tbody>
</table>

DRAC → Dell Remote Access Card

Alternatively if there are not enough physical NICs, one could accomplish this by using VLANs. We also need to configure redundancy at the vSwitch and at the physical switch level.
Storage

According to the inventory report from the capacity planner we need a Storage Area Network [SAN] with at least 53 TB usable disk space. A SAN is typically used in vSphere environments such that datastores can be shared across all the servers in the vSphere farm. vSphere features such as VMware High Availability, Distributed Resource Scheduler and VMware Fault Tolerance depends on shared datastores.

Since our company AMG is predominantly a dell shop, consisting of Dell servers, desktops, laptops, printers and tape drives, management decided to go with a storage solution from Dell. An iSCSI SAN is preferred over Fiber channel because of the following reasons

- AMG’s existing TCP/IP network infrastructure can be leveraged to easily deploy iSCSI Storage Area Network [SAN]
- Use of a fiber channel SAN would require AMG to procure additional hardware such as Host Bus Adapters for servers which communicate to the fiber channel SAN through the fiber channel switches via fiber cables.
- iSCSI SANs can be implemented without any investment in training personnel to implement and configure fiber channel SAN
- 10 Gig Ethernet is around the corner, which can carry data at faster speeds compared to today’s 8 Gig Fiber Networks.

For the purposes of this project Dell Equallogic PS6510E is chosen. The storage units at the primary data center and DR site are configured as master and slave respectively. Replication is tested between the primary data center and DR site.

Sample Capacity Planner

<table>
<thead>
<tr>
<th>Scenario Name</th>
<th>Systems Analyzed</th>
<th>ESX Hosts Required</th>
<th>System Exceptions</th>
<th>Overall Consolidation Ratio %</th>
<th>Total Storage Required (TB)</th>
<th>Rack Used</th>
<th>KW Used</th>
<th>Tons BTU/hr Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell Conservative Scenario</td>
<td>9</td>
<td>3</td>
<td>2</td>
<td>44</td>
<td>0.852</td>
<td>7</td>
<td>1.09</td>
<td>4,548.60</td>
</tr>
<tr>
<td>Dell Moderate Scenario</td>
<td>9</td>
<td>2</td>
<td>1</td>
<td>67</td>
<td>0.95</td>
<td>4</td>
<td>0.04</td>
<td>2,600.00</td>
</tr>
</tbody>
</table>

Courtesy: Dell
**Global Traffic Managers**

Global Traffic Managers [GTM] redirect network traffic automatically among VMs spread across multiple data centers. Thus in an event of a disaster at the primary data center network traffic is automatically rerouted to the DR site. For this project we are going to place the GTMs in front of the firewall at primary data center and DR locations respectively. Doing so we leverage features such as WAN optimization, web acceleration and automatic failover and failback between primary data center and DR locations.

As an example, here are the following steps taken by a client on the internet to resolve a Domain Name System [DNS] server query to our web site.

- Clients query local DNS servers.
- Local DNS server then queries Start of Authority [SOA] DNS servers. Every domain has a SOA record in its DNS database. Amongst other information, SOA record consists of hostname for the primary DNS server and the secondary DNS servers, which in our case are located at the primary data center and the DR site respectively.
- SOA DNS servers query the GTM for global availability.
- GTM always returns DNS “www record” entry for primary data center; if primary data center is unavailable then GTM returns the DNS “www record” for the DR site.

In such situations where primary data center is unavailable, the GTM not only directs clients to access the web servers in the DR site but also the applications in the DR site receive the same availability and performance benefits from the GTM as the applications in the primary data center did.

Now we need to choose a model of GTM that will be sufficient for our needs today and growth tomorrow, keeping in mind that the network bandwidth in the primary data center and in the DR site which are 25mbps full duplex and 10 mbps full duplex respectively.

The following is a comparison chart between different models of BIG-IP f5 GTMs.
Platform Performance for LTM

<table>
<thead>
<tr>
<th></th>
<th>BIG-IP 1600</th>
<th>BIG-IP 3600</th>
<th>BIG-IP 3900</th>
<th>BIG-IP 6900</th>
<th>BIG-IP 8900</th>
<th>VIPRION With 4 blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. throughput</td>
<td>1 Gbps</td>
<td>2 Gbps</td>
<td>4 Gbps</td>
<td>6 Gbps</td>
<td>12 Gbps</td>
<td>40 Gbps</td>
</tr>
<tr>
<td>Layer 4</td>
<td>60,000</td>
<td>115,000</td>
<td>175,000</td>
<td>220,000</td>
<td>400,000</td>
<td>1 Million</td>
</tr>
<tr>
<td>Layer 7</td>
<td>100,000</td>
<td>135,000</td>
<td>400,000</td>
<td>600,000</td>
<td>1,200,000</td>
<td>3,200,000</td>
</tr>
<tr>
<td>Request/sec (Inf-inf)</td>
<td>4 Million</td>
<td>4 Million</td>
<td>8 Million</td>
<td>8 Million</td>
<td>16 Million</td>
<td>32 Million</td>
</tr>
<tr>
<td>Max. conc. conn.</td>
<td>5,000</td>
<td>10,000</td>
<td>15,000</td>
<td>25,000</td>
<td>58,000</td>
<td>200,000</td>
</tr>
<tr>
<td>Max. SSL TPS</td>
<td>1 Gbps</td>
<td>1.5 Gbps</td>
<td>3.8 Gbps</td>
<td>4 Gbps</td>
<td>9.6 Gbps</td>
<td>36 Gbps</td>
</tr>
<tr>
<td>Max. SSL Bulk</td>
<td>1 Million</td>
<td>1 Million</td>
<td>1 Million</td>
<td>2 Million</td>
<td>4 Million</td>
<td>8 Million</td>
</tr>
<tr>
<td>Max. SSL conc. conn.</td>
<td>750 Mbps</td>
<td>1 Gbps</td>
<td>3.8 Gbps</td>
<td>5 Gbps</td>
<td>8 Gbps</td>
<td>16 Gbps</td>
</tr>
<tr>
<td>Switch backplane</td>
<td>14 Gbps</td>
<td>24 Gbps</td>
<td>34 Gbps</td>
<td>68 Gbps</td>
<td>112 Gbps</td>
<td>368 Gbps</td>
</tr>
</tbody>
</table>

Courtesy: [http://www.f5.com](http://www.f5.com)

Hence we chose f5-BIG-IP1600 which is more than sufficient for our needs; any other model would probably be overkill.

The following diagram represents a high level overview of the networking infrastructure with redundant routers, GTMs, firewalls and switches setup at the primary data center and the DR site respectively.
Planned Environment

Primary Data Center

- Trusted Connection
- (Router)
- (Global Traffic Manager)
- (Firewall)
- (Ethernet Switch)
- Storage-1
- Replication
- Dedicated Internet

DR Site

- Trusted Connection
- (Router)
- (Global Traffic Manager)
- (Firewall)
- (Ethernet Switch)
- Storage-2
- Replication
- Dedicated Internet

Index
- Sync
- Stand By
The P2V process

For the process of converting a physical server into a virtual server [also known as P2V] we can use VMWare vCenter Convertor. There are also a number of 3rd party utilities which can convert a physical server to a virtual server. Some of them are

- vConvertor from VisionCore Inc
- PlateSpin Migrate from Novell

These products will create an initial snapshot and continue to take block level updates at scheduled intervals, until appropriate time to cut over when we synchronize one last time before allowing vConvertor or PlateSpin to convert to VMware format and present to the vSphere servers.

VMware Site Recovery Manager (SRM)

SRM helps our organization to quickly failover and failback during a disaster. It is an add-on software from VMware. For our business needs we purchased SRM licenses for both primary data center [protected site] and DR sites [recovery site].
Pre-installation steps to be performed on primary data center [protected site] and DR [recovery site]

I. SRM does not create a new database during installation, we have to create one manually on the SQL server. In our case I named the database “SRM” and gave the user account “vCenteradmin” permissions as “db_owner”.

II. Next we need to install the storage replication adapters on each vCenter server located at the Primary data center and the DR site respectively. Storage replication adaptor works with SRM to replicate data between the SANs to and from the primary data center and DR site respectively with full transactional integrity. This installation package is dependent on the vendor from whom we procure the SAN. The Dell EqualLogic SRA can be downloaded from the VMware website.
Install SRM on the vCenter server in the Primary Data Center.

i. Launch the installation package and follow the wizard. When prompted with following screen, enter the Fully Qualified Domain Name of the vCenter server, authorized username and password.

![Image of VMware Site Recovery Manager registration screen]

ii. When prompted to choose a certificate method for authentication choose “Automatically generate a certificate”

![Image of Certificate Type Selection]
iii. On the next prompt I associate the ip of vCenter server at the primary data center with a friendly name. I have called it “Protected Site at Primary Data Center”

![Image of VMware Site Recovery Manager]

iv. On the next screen we are prompted to enter the details for the SRM database. Click “Add”

![Image of VMware Site Recovery Manager with SQL Native Client selected]

Choose “SQL Native Client”
On this screen type the name of the SRM database created during the pre-installation step, give it a friendly name and choose the server that SRM database resides on.

Choose SQL authentication, enter the authorized user id and password.
Verify that Default Database is SRM

Click Next
One last step before installation begins. Type the data source name along with the authorized database user name and password.

Click Next & Install.

Install SRM on the vCenter server at the DR Site

We install SRM with site recovery adapters on the vCenter server at the DR site following the same procedures above.

Post installation steps to configure SRM and create recovery plan for failover to DR site

A. After logging on to the vCenter through vSphere Client the following steps are performed at the primary data center
   
a. Enable the SRM plug-in and follow the install wizard
b. Configure “Connection”, “Array Managers” and “Inventory Mapping” by clicking on Site Recovery Button on the vCenter console.
   i. Start by clicking on site recovery
   
   ![Site Recovery Button](image)

   ii. Click Configure and follow the guided wizard.

B. Before we create a “Protection Groups” it is important to consider Recovery Time Objective [RTO] and Recovery Point Objective [RPO]. Accordingly the servers, based on their roles have been classified into one of the following categories.
   i. Core infrastructure
   ii. Mission critical
   iii. Non-critical
   iv. Not protected.

Mail, Citrix, Active Directory, web and database servers have each their own “Protection Group”. This will help us failover/failback individual servers based on their roles during a disaster.

C. Configure recovery plan at the DR site.
   a. Connect to the vCenter Server located at DR site. Under “Site Recovery“. Verify the entries for Local and Paired sites.

Definitions

**Recovery Point Objective** (RPO) describes the acceptable amount of data loss measured in time

**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. Source: [http://en.wikipedia.org/wiki/Recovery_time_objective](http://en.wikipedia.org/wiki/Recovery_time_objective)
b. Configure “Array Managers” and “Inventory Mapping” the same way we did on the vCenter at the primary data center.

c. Create “Recovery Plans”, for each protection group.

Testing the recovery plan from the DR site

A. For each recovery plan verify and make changes if necessary by editing “Recovery Plans”. In our circumstance we need to change IP addresses and change the order in which, each server boots.

The following screenshot shot the recovery plan in detail.

B. Now it is time to test the failover from the primary data center to the DR site. Click Test in the upper left hand corner, which will simulate failover to the DR site without affecting the production network.
When everything goes right, we see the following message.

![Message]

Configure SRM and create recovery plan for failback to primary data center.

A. Connect to the vCenter Server located at primary data center.
B. Configure “Recovery Plans” for each protection group at the primary data center.
C. For each recovery plan verify and make changes if necessary by editing “Recovery Plans”. In our circumstance we need to change IP addresses and change the order in which, each server boots.

Testing the failback from the DR site

A. Reverse the replication roles such that the storage units at the primary data center and DR site are configured as slave and master respectively.
B. Replication is tested between the primary data center and DR site.
C. Verify that the data between the two SANs located at Primary Data Center and the DR site is identical.
D. Click “Run” to visualize the real failback in action.

![Run]

Thus to failover or failback a single or multiple protection groups, all we need is a click.

I call this a one touch Disaster Recovery solution.

**Project Timeline**

Each server has been classified into five different groups, for example since we have five Citrix servers, each Citrix server has been placed in a group, similarly each web server has been placed in a group. So a typical group consists of servers of varying roles ranging from file, print, web, Active Directory, SQL servers etc. Following this plan there is a seamless transition when virtualizing the servers which means that there would be no downtime.
The following is the time line of the project.

<table>
<thead>
<tr>
<th>Month</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Month 1</td>
<td>Run VMware Capacity Planner</td>
</tr>
<tr>
<td></td>
<td>Purchase Networking, storage and VMWare Licenses</td>
</tr>
<tr>
<td>Month 2</td>
<td>Configure Networking Storage and VSphere Servers in the Data Center and DR location</td>
</tr>
<tr>
<td></td>
<td>Setup Replication between the storage units</td>
</tr>
<tr>
<td>Month 3</td>
<td>Virtualize Group 1</td>
</tr>
<tr>
<td></td>
<td>Test</td>
</tr>
<tr>
<td>Month 4</td>
<td>Virtualize Group 2</td>
</tr>
<tr>
<td></td>
<td>Test</td>
</tr>
<tr>
<td></td>
<td>Setup Site Recovery Manager</td>
</tr>
<tr>
<td></td>
<td>Test Fail Over and Failback with the servers virtualized during Month 3</td>
</tr>
<tr>
<td>Month 5</td>
<td>Virtualize Group 3</td>
</tr>
<tr>
<td></td>
<td>Test</td>
</tr>
<tr>
<td></td>
<td>Test Fail Over and Failback with the servers virtualized during Month 4</td>
</tr>
<tr>
<td>Month 6</td>
<td>Virtualize Group 4</td>
</tr>
<tr>
<td></td>
<td>Test</td>
</tr>
<tr>
<td></td>
<td>Test Fail Over and Failback with the servers virtualized during Month 5</td>
</tr>
<tr>
<td>Month 7</td>
<td>Virtualize Group 5</td>
</tr>
<tr>
<td></td>
<td>Test</td>
</tr>
<tr>
<td></td>
<td>Test Fail Over and Failback with the servers virtualized during Month 6</td>
</tr>
<tr>
<td>Month 8</td>
<td>Test Fail Over and Failback with the servers virtualized during Month 7</td>
</tr>
<tr>
<td></td>
<td>Draft a Disaster Recovery Plan</td>
</tr>
<tr>
<td>Month 9</td>
<td>Test Disaster Plan with a scheduled fail over to DR site</td>
</tr>
<tr>
<td></td>
<td>Continue to draft a Disaster Recovery Plan</td>
</tr>
<tr>
<td>Month 10</td>
<td>Finalize the Disaster Recovery Plan</td>
</tr>
<tr>
<td></td>
<td>Test Disaster Plan with an unscheduled fail over to DR site</td>
</tr>
<tr>
<td></td>
<td>Final Review of the Disaster Recovery and Business Continuity Plan with Management for approval</td>
</tr>
</tbody>
</table>
Concluding Remarks:

Following the above plan we have

I. Designed and tested **One Touch disaster recovery plan** with ease without bringing down the production network.

II. Leveraged technologies such as data de-duplication and compression on GTMs, thereby reducing the amount of data that is sent across for replication, which in turn **reduces transfer time and bandwidth needed**.

III. Consolidated servers, eliminated the need for ongoing data center expansion, slashed power costs and **reduced the total cost of ownership**.

IV. Made the **maximum use of the available server hardware** by sharing it across multiple applications, thereby maximizing ROI

V. Implemented a plan which is easy to manage and scalable for future growth, resulting in **reduced administrative burden**.

VI. **Compliance** with various Federal Computer Acts and Standards such as HIPPA and SAS 70 respectively

VII. An **easier, faster and consistent** centralized server deployment and protection of Virtual Machines.

VIII. Devised a solution where test, development and upgrade on production can be accomplished **without any downtime**

IX. Significantly **slashed the carbon emissions** from our Data Centers.

X. **Eliminated single point of failure at the Data Center level.**

   Getting trained and certified in VMware, Microsoft, f5 and Cisco $20,000,
   Obtaining hardware and software for the One Touch DR project $300,000,
   Having an sound sleep because you have a time tested Disaster Recovery Plan priceless!

Thus unlike traditional disaster recovery methods which are often labor intensive, error prone and slow; virtualization provides a fast, reliable and the most cost effective solution.
Glossary of Acronyms

COOP   Continuity of Operations
DMZ    Demilitarized Zone
DNS    Domain Name Service
DR     Disaster Recovery
DRS    Distributed resource scheduler
GTM    Global Traffic Managers
HIPAA  Healthcare Information Portability and Accountability Act of 1996
RPO    Recovery Point Objective
RTO    Recovery Time Objective
SAN    Storage Area Network
SOA    Start of Authority
SRM    VMware Site Recovery Manager
VM     Virtual Machine
VMHA   VMware High Availability
**Bibliography**

Figures 1 through 8 are courtesy of VMware.com

Parts of the network diagram on Page 18 is created using the official VMware icon and diagram library located at [http://communities.vmware.com/servlet/JiveServlet/download/12204-1-36063/PPT_Library_VMware_icons-diagrams_Q409_COMM.pptx](http://communities.vmware.com/servlet/JiveServlet/download/12204-1-36063/PPT_Library_VMware_icons-diagrams_Q409_COMM.pptx)

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at [http://www.vmware.com/go/patents](http://www.vmware.com/go/patents). VMware does not endorse or make any representations about third party information included in this document, nor does the inclusion of any VMware icon or diagram in this document imply such an endorsement. [http://communities.vmware.com/docs/DOC-12204]

*All other trademarks and copyrights are property of their respective owners.*
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Las Vegas Summer 2020</td>
<td>Las Vegas, NV</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Silicon Valley - Cupertino 2020</td>
<td>Cupertino, CA</td>
<td>Jun 22, 2020 - Jun 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Chicago Spring 2020</td>
<td>Online ILUS</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>