Documenting: Virtual Design Master – Challenge 3

Presented to: Messrs. Virtual Design Master Judges

Ref: AA-vDM-03-03

Prepared by: Abdullah Abdullah

Lebanon, Beirut

Twitter: @do0dzZZ
Blog: http://notes.doodzzz.net

E-mail: abdullah@lowerlayer.net

[Synopsis]

While things on Mars have been going well, since we now have multiple options for our infrastructure, the fact remains that we are working on the colonization of a foreign planet. We all know disasters can happen, after all, Mars is quite dusty. What happens if someone leaves the door to the data centre open during a dust storm? What happens if inter site communications go down during a dust storm or a solar storm? We need to make sure we are planning for every contingency.

While a great deal of time and energy is being spent working on Mars right now, we can't forget our colony on the Moon, which is a perfect choice for disaster recovery. There is an advanced laser communications link between the Moon and Mars, with a consistent latency of under 10 milliseconds no matter what time of day it is. Like on Mars, our billionaire friend is also planning to build a public cloud infrastructure on the Moon.

Your challenge is to come up with a disaster recovery plan for our key applications on Mars. The components you need to protect are as follows:

- 5 node Microsoft Exchange environment (2 front---end and 3 mailbox servers). Each machine with 4 CPU and 12 GB of RAM.
- 15 web application servers running IIS/MSSQL locally on each instance. Each machine is 2 CPU and 8 GB of RAM.
- 3 servers running a MariaDB cluster. Each machine with 1 CPU and 4 GB of RAM.
- 5 file servers (15 TB each of storage). Each machine with 2 CPU and 12 GB of RAM.
- 15 virtual machines running CoreOS to support Docker. Each machine with 4 CPU and 12 GB of RAM.\
- 2 legacy Windows NT 4 servers running IBM DB2. Each machine with 1 CPU and 4 GB of RAM.

In addition, you must define the RTO and RPO you plan on using for each application, and why. Show what products you would use for this disaster recovery scenario, and what processes and procedures would be used in a disaster. You may build a new infrastructure on the Moon, or use any public cloud infrastructure. Be sure to clearly justify the choices you are making.

Table of Contents

1. Executive Summary

1.1. Project Overview

As we delve more into technology and the needs of the colony we realize that as maintainers of the IT infrastructure our tasks are endless and our projects are limitless.

Now that Mars has its IT infrastructure scoped and fully functional we have put on our gloomy hat and we're thinking again about survival (lessons learned from earth), we need to establish a way of keeping things running even if some other alien fellows wanted to acquire the planet, or if for any reason Mars had a major change in its environment forcing us to leave!

Our focus will be on creating our Business Continuity Plan (BCP) covering all of its aspects including the Disaster Recovery Plan (DRP).

1.2. Intended audience

This document is intended for those involved in the BCP and DRP and to anyone who will take part in testing or fulfilling the BCP and DRP if the worse has come to pass.

1.3. Project Insights

Our Business Continuity Plan with be a combination of both hardware and software technologies that will be carefully designed and configured to meet our requirement.

Because our systems are supporting the whole colony which is increasing and advancing we will be having a BCP that protects us against planetary failure.

Our disaster site will be on our beloved earth moon where the human race were given another chance at survival (even though we didn't have BCP for us as humans at that time ;-)).

1.3.1. Project Requirement

- R001: Protect the Microsoft Exchange environment.
- R002: Protect the web application servers running IIS/MSSQL.
- R003: Protect the MariaDB cluster.
- R004: Protect the file servers.
- R005: Protect the virtual machines running CoreOS thar supports Docker.
- R006: Protect the legacy Windows NT 4 servers running IBM DB2.
- R007: Utilize the moon as the DR site.

1.3.2. Project Constrains

- C001: NT systems are no longer supported by its vendor (Microsoft)
- C002: 75TB of file server storage is a challenging number in terms of initial full replication.

1.3.3. Project Assumptions

- A001: The disaster site will need to serve 50% of the users.
- A002: Qualified personnel are available on both Mars and Moon to carry out the BCP.
- A003: The laser equipment that has been setup is error-free and redundant against device failure.
- A004: All services servers are virtual machines none of them are physical servers.
- A005: The public cloud infrastructure is not ready and needs planning/building.
- A006: The administration team is most knowledgeable with VMware technologies.
- A007: Plenty of hardware available on Earth's Moon.
- A008: The MariaDB cluster is a Galera Cluster.
- A009: The total storage for the workload that needs to be protected excluding the file servers is around 15TB.
- A010: The file servers storage is an enterprise class NAS.

1.3.4. Protection Assumptions

While we do not have the full capability on doing a pilot to specify the exact RTO and RPO that we need to achieve, hereunder is a table representing our assumptions:

Workload	Value	Availability	RPO (Data Loss Risk)	RTO (Disaster Site)	RTO (Protection Site) – Minimum
Directory Services	Productivity important	99.999%	15 minutes	None	- Database 2 hours. - GRT 15 minutes.
Exchange Environment MBX	Productivity important	99.999%	5 minutes	None	- Database 1 day (depending on the database size). - GRT 2 hours.
Exchange Environment CAS	Productivity important	99.999%	0 minutes	None	N/A
Web Application Servers	Productivity important	60%	15 minutes.	25 minutes	N/A
MariaDB	Productivity important	99.999%	0 minutes	None	- Database 2 hours.
File Servers	Productivity important	99.999%	15 minutes	None	- Depends on the files that require recovery (30 minutes to days).
CoreOS w/ Docker	Productivity important	70%	15 minutes.	25 minutes	N/A
NT4 w/ IBM DB2	Productivity important	50%	15 minutes.	25 minutes	N/A

2. Design Summary

When dealing with disaster recovery most of the time the decision to failover to the disaster site comes from the highest managerial position, of course the people in-charge of relaying this information are the IT people especially when there is data loss involved.

2.1. Disaster Recovery Sites

From our experience in terms of decreasing the RTO we would implement the availability at the application level whenever it's supported.

Because we are paranoid when it comes to disaster and because we have experienced the pain from the drastic events that happened on Earth, we will utilizing two solutions to achieve a complete BCP.

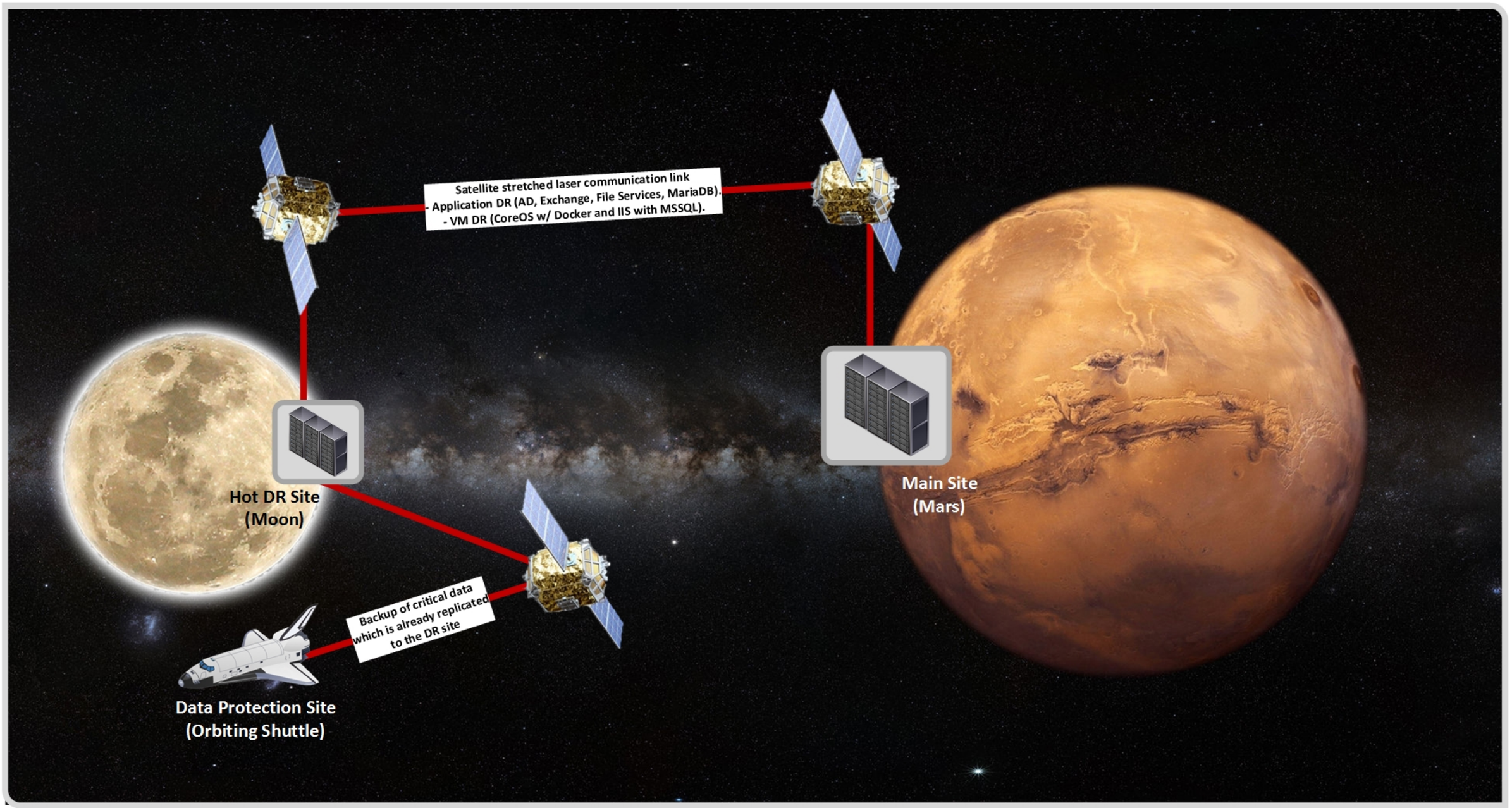
So the design decision will be as follow:

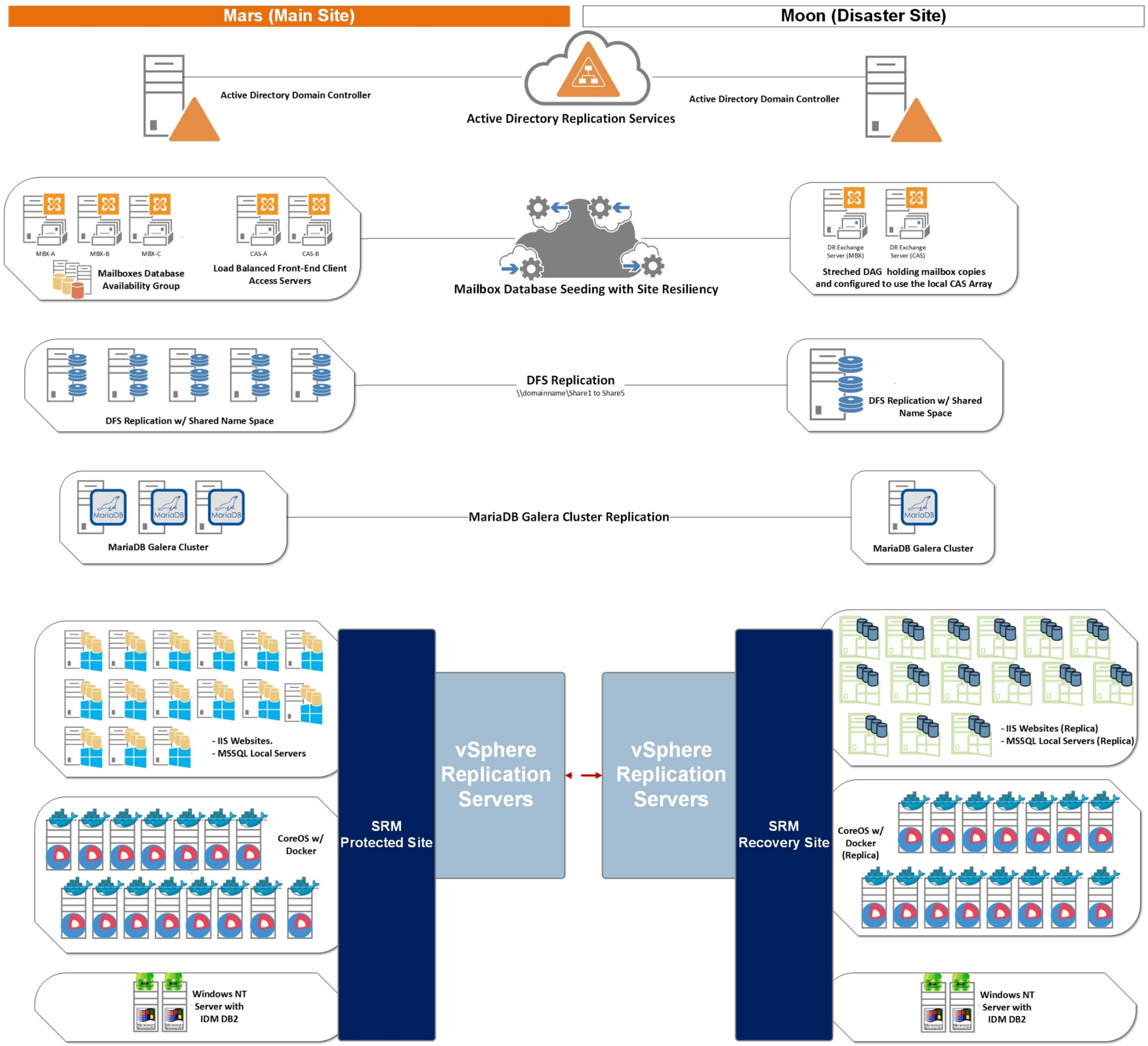
1- Since the public cloud is not ready and we need to get the DR site up and running as soon as possible we will not go down that path.

2- **Hot DR Site** (A datacenter on Earth's Moon): We will be clearing one of the datacenters on the Moon so that to be utilized as our hot disaster recovery site.

3- **Data Protection Site**: For us it is just not enough to even have hot DR site, what is the Moon fails for some reason? Well for that purpose we will be utilizing one of our spaceships, it will be complete overhauled to function as an orbital datacenter which will host a backup of the critical data that can't be rebuilt and is vital to our survival as a race.

The up above will bring us close to our desired protection and service wise availability.


Satellite stretched laser communication link
- Application DR (AD, Exchange, File Services, MariaDB).
- VM DR (CoreOS w/ Docker and IIS with MSSQL).
Hot DR Site
(Moon)
Main Site
(Mars)
Backup of critical data
which is already replicated
to the DR site
Data Protection Site
(Orbiting Shuttle)


Mars (Main Site)
Moon (Disaster Site)
Active Directory Domain Controller
Active Directory Replication Services
Active Directory Domain Controller
MBX-A
MBX-B
MBX-C
Mailboxes Database Availability Group
CAS-A
CAS-B
Load Balanced Front-End Client Access Servers
Mailbox Database Seeding with Site Resiliency
DR Exchange Server (MBX)
DR Exchange Server (CAS)
Streched DAG holding mailbox copies and configured to use the local CAS Array
DFS Replication w/ Shared Name Space
DFS Replication
\\domainname\Share1 to Share5
DFS Replication w/ Shared Name Space
MariaDB Galera Cluster
MariaDB Galera Cluster Replication
MariaDB Galera Cluster
- IIS Websites.
- MSSQL Local Servers
CoreOS w/ Docker
Windows NT Server with IDM DB2
SRM Protected Site
vSphere Replication Servers
vSphere Replication Servers
SRM Recovery Site
- IIS Websites (Replica)
- MSSQL Local Servers (Replica)
CoreOS w/ Docker (Replica)
Windows NT Server with IDM DB2

To summarize the up above diagrams, in terms of disaster recovery we have something for each type of workload:

1- Active Directory, DNS services will be replicated via AD FRS utilizing another domain controller on Moon.
2- For Exchange MBX, we will be stretching the database availability group and leverage lagged log replay in the recovery site.
3- For Exchange CAS (front-end), we will be extending the load balanced front-end servers and add to them a standby server in the DR site.
4- For the file servers: we will be utilizing DFS replication with a shared name space this will be detailed later on in another dedicated section.
5- For the MariaDB cluster, we will be adding two additional nodes in DR leveraging the Galera cluster replication.
6- For the standalone servers (MSSQL/IIS, CoreOS/Docker and Windows NT w/ DB2) we will be leveraging VMware Site Recovery Manager (SRM).
7- For additional data protection site we will be utilizing Symantec Backup Exec to perform backup of workloads that hold our critical data, this will be detailed in the backup section.

2.2. Hot DR Site (The Moon Datacenter)

2.2.1. Physical and Logical Designs

In terms of physical design in a high level view we have workloads requiring performance and we have workloads that require only storage, as such we will be having:

1- VSAN clusters that will be used.
2- An enterprise class NAS device with NFS datastores to host the data of the file servers.
3- We have plenty of 10Gbps switches which will serve us to build the datacenter.

According to our design the DR must support the following production workloads:

Virtual Machine	# of VMs	Description	CPU	Memory
Domain Controller	1	AD Domain Controller	2 vCPU	4GB
Exchange Server – MBX	1	Exchange Mailbox Role	6 vCPU	24GB
Exchange Server – CAS	1	Exchange Front-End Role	4 vCPU	12GB
File Server	1	File Server	4 vCPU	16 GB
MariaDB Cluster Node	1	DR Cluster Node	1 vCPU	4GB
IIS/MSSQL	15	Various web applications running on different servers each with its standalone database engine.	30 vCPU	120GB
CoreOS with Docker	15	Docker containers running separately on each CoreOS	60 vCPU	180GB
Windows NT with DB2	2	Legacy Windows NT servers with IBM DB2	2 vCPU	8GB
Total	**37**		**109 vCPU**	**368GB**

The DR infrastructure has a management cluster as well, and it consists of:

Virtual Machine	Description	CPU	Memory
VMware vCenter Server	DR Site Virtual Center Server	2 vCPU	8GB
vCenter SRM Server	DR Site Recovery Manager Server	2 vCPU	4GB
vCenter Replication Server	DR Site Replication Server Engine	4 vCPU	4GB
MSSQL Database Server	MSSQL Database for vCenter and SRM Servers	2 vCPU	8GB
Total		**10 vCPU**	**24GB**

To able to provide our DR data center with its compute, storage and network requirements we have decided to build the hereunder VSAN nodes from the hardware that we found available:

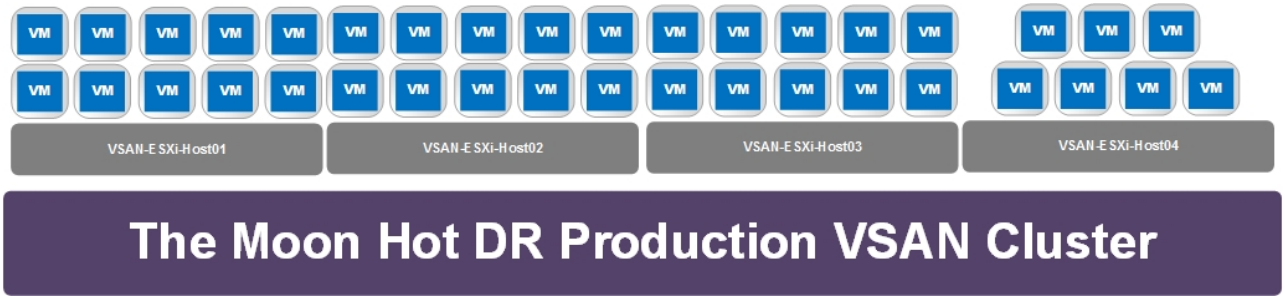
2.2.2. DR Production Cluster

Components	Details	QTY
System	VSAN Cluster Node	1
Processor	Intel® Xeon® E5-2650 v2 (2.6GHz/8-core/20MB)	2
Memory	16GB chips	16
SSD	200GB Solid State Drive	2
Raw Data Disks	1TB SAS 7.2k Hard Drive	8
RAID Controller	LSI 3008 based controller	1
Ethernet	10Gb2-port adapter	1
SD Card	8GB SD Card (we will use this card to install the ESXi OS on)	1

Our production cluster will consist of **4 VSAN nodes**, giving us the following capabilities:

Components	# of Nodes	# of HDDS	# of SSD	Raw Disk Capacity
VSAN Cluster	4	32	8	32

Components	VM tolerance per node	# of disk groups	# of disks per disk group	Raw Disk Capacity	Host failure tolerance
VSAN Cluster	10	8	4	32	1



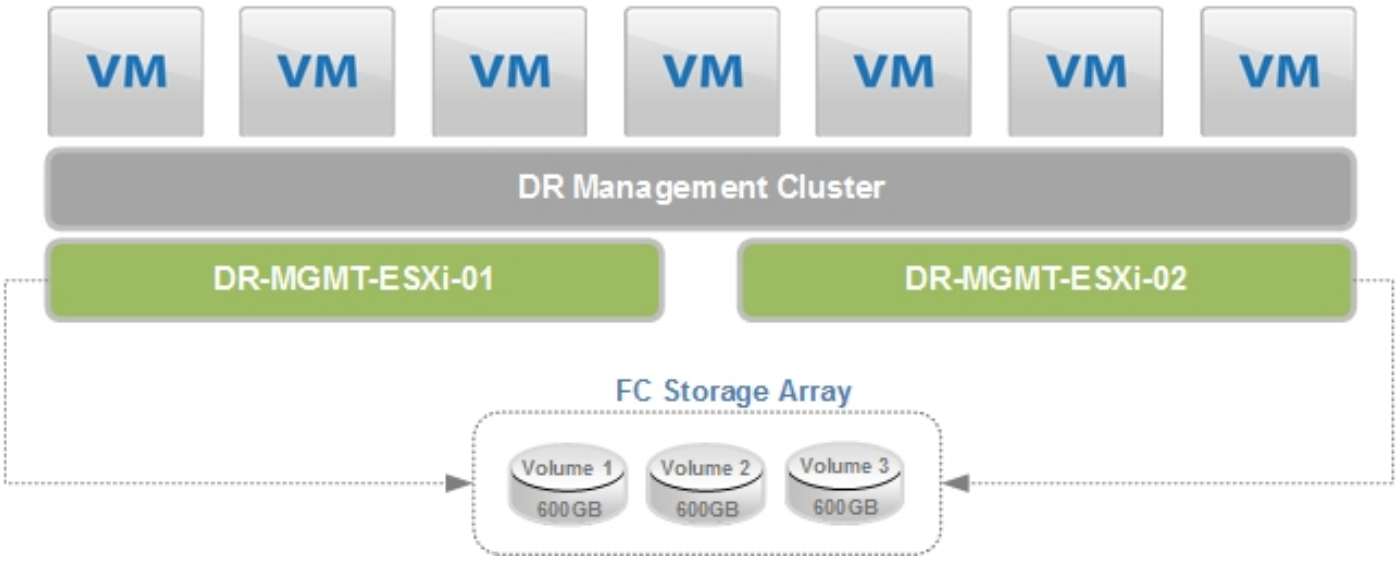
The up above sizing should be sufficient to serve our production workload in the DR site with additional resources saved in case additional workloads are to be protected as well.

2.2.3. DR Management Cluster

Because our management cluster has a lower requirement than that of the production, we were lucky enough to find a legacy FC storage that has around 2TB of capacity and we will incorporate into our design:

Components	Details	QTY
System	Management Node	1
Processor	Intel® Xeon® E5-2630L v2 (2.4GHz/6-core/15MB)	2
Memory	16GB chips	8
HBA	FC 8Gbps 2-port adapter	1
SD Card	8GB SD Card (we will use this card to install the ESXi OS on)	1

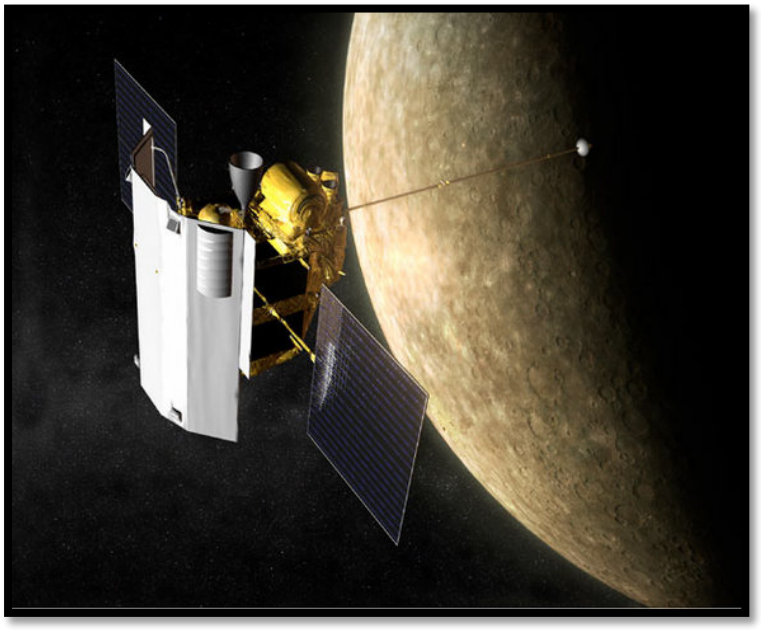
To be able to support our workload, the high availability requirement our management cluster will be consisting of two nodes that will be connected back to back to the FC storage thus there will be no need to have an FC switch.



2.2.4. DR Networking

LAN: We will be utilizing the 10Gbps switches that we have for both the production cluster and management cluster.

WAN: Our reliable inter-satellite network covering the distance between Earth's Moon and Mars will serve us well in terms of transferring our data back and forth between the Main Site and DR Site, early tests that were performed had shown that the data passing rate is around 622Mbps.



In addition we will be utilizing stretched VLANs and not VLAN islands so that to minimize the reconfiguration of components in terms of networking, reducing the complexity and giving us more control over our RTO.

2.2.5. Mars Management Cluster Additional Components

The datacenter back in mars will have these additional components added to it:

Virtual Machine	Description	CPU	Memory
vCenter SRM Server	Main Site Recovery Manager Server	2 vCPU	4GB
vCenter Replication Server	Main Site Replication Server Engine	4 vCPU	4GB

2.3. Workloads Protection

2.3.1. Exchange Servers

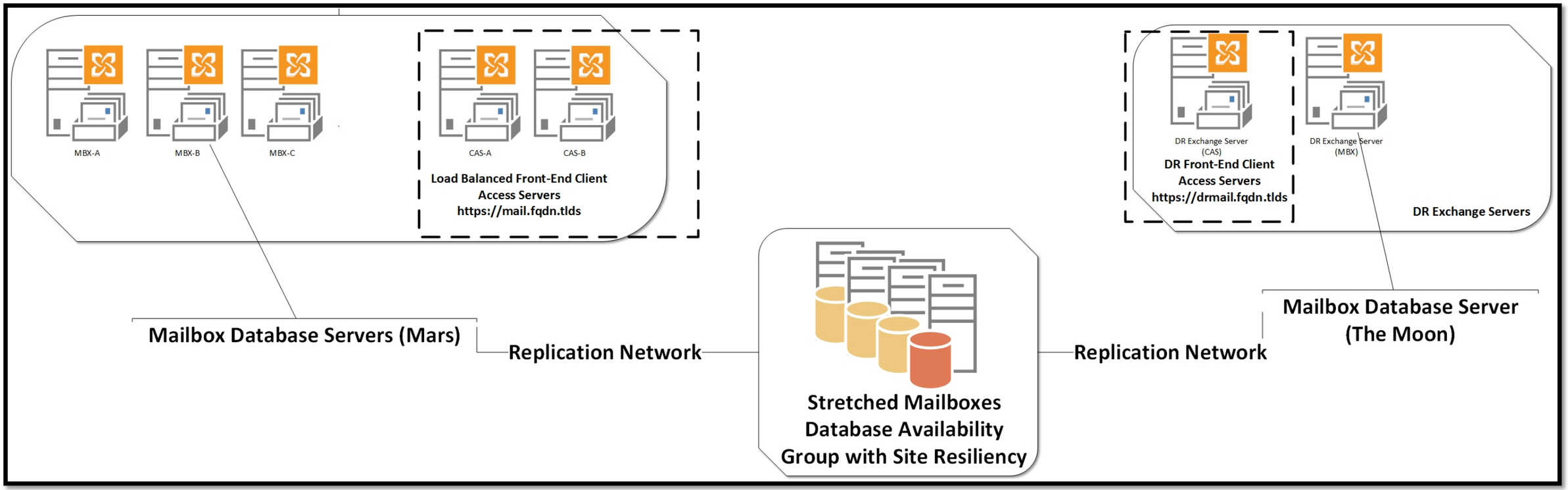
The Exchange Servers is one of the most vital systems that we rely on for communication between each other, this workload on Mars has been protected at the application level utilizing multiple mailbox servers to hold database copies and multiple client access servers to handle users front-end access.

Utilizing the same technology we will be extending the protection of our Exchange environment to the disaster site.

Hereunder you'll find the process to switch over to the DR site and what needs to be done for each of the roles covered:

1- 1 Mailbox server to hold passive copies of all the databases:
- **a.** A lagged mailbox database copy is a mailbox database copy configured with a replay lag time value greater than 0.
- **b.** Activating and recovering a lagged mailbox database copy is a simple process if you want the database to replay all log files and make the database copy current.
- **c.** Estimated time to complete this task: 1 minute, plus the time it takes to duplicate the lagged copy, replay the necessary log files, and extract the data or mount the database for client activity.

2- 1 Client Access server to handle all user requests:
- **a.** Most of the configuration is held in Active Directory database and we have a second domain controller replicating its databases from Mars to the Moon.
- **b.** Some configuration needs to be explicitly made such as Receivers and Certificates.
- **c.** Access of the mailboxes in the DR site will be via Outlook Web Access through this URL https://drmail.fqdn.tlds
- **d.** No other front-end services will be provided.


MBX-A
MBX-B
MBX-C
CAS-A
CAS-B
Load Balanced Front-End Client Access Servers
https://mail.fqdn.tlds
DR Exchange Server (CAS)
DR Front-End Client Access Servers
https://drmail.fqdn.tlds
DR Exchange Server (MBX)
DR Exchange Servers
Mailbox Database Servers (Mars)
Replication Network
Stretched Mailboxes Database Availability Group with Site Resiliency
Replication Network
Mailbox Database Server (The Moon)

Monitoring the DAG health can be done via the Exchange Administration Console or via running Powershell scripts and scheduling them to be emailed on a daily basis, the script can be found in Appendix A.

2.3.2. File Servers

Well we're in space! People like to take pictures and document maps and we have all the data related to the trips and findings on Mars and these all needs to go back to the Moon, this is the legacy of humans and can't be lost at any cost.

So we have 5 file servers, each file server has around 15TB of storage totaling 65TB of storage, performing a storage replication in our infrastructure is feasible but it will have an immense effect on our RTO, the files must be available for access at any time! What if a spaceship got lost and we need one of our charted maps to guide it.

So the design decision was to install an enterprise NAS in the DR site with an NFS share, with 1 VM acting as a file server and it will be the NFS client.

To get all of our files to the Moon DR we will be utilizing Microsoft DFS replication with a shared name space such as:

- \\domainname\Share1 < This comes from File Server 1.
- \\domainname\Share2 < This comes from File Server 1.
- \\domainname\Share3 < This comes from File Server 1.
- \\domainname\Share4 < This comes from File Server 1.
- \\domainname\Share5 < This comes from File Server 1.

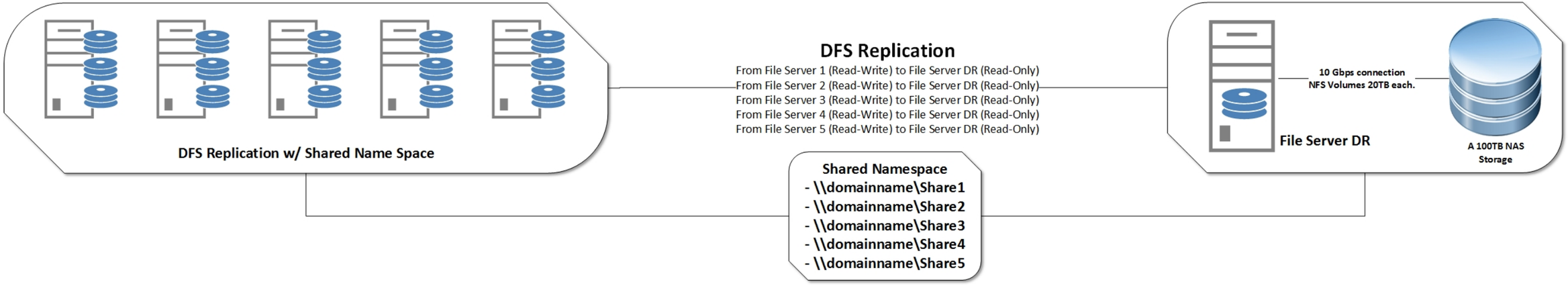
We will have 5 replication groups, each group will be configured as follows:

1- A multipurpose replication group.
2- A full mesh topology (will be needed if we want to reverse the replication).
3- Full bandwidth.
4- Schedule will be all with a 12 hours duration.
5- The replicated folders on the Moon DR will be read-only so that no to have any conflicts in our files whatsoever.

Before beginning the replication and since we have around 65TB of already occupied storage we will be performing an offline seeding of the existing file to the DR site on the Moon because the initial replication would take ages and ages considering the enormous size of the data.

We will bring the DR NAS from the Moon to Mars (round trip around 500 days) copy the data and then enable the replication, details on how to configure offline seeding can be found in appendix B.

Sadly although DFS is efficient and can do the job it lacks proper built-in monitoring, we will be utilizing a PowerShell script that will be schedule to run on a daily basis to provide us with the required details on DFS replication, the script can be found in appendix C.


DFS Replication w/ Shared Name Space
DFS Replication
From File Server 1 (Read-Write) to File Server DR (Read-Only)
From File Server 2 (Read-Write) to File Server DR (Read-Only)
From File Server 3 (Read-Write) to File Server DR (Read-Only)
From File Server 4 (Read-Write) to File Server DR (Read-Only)
From File Server 5 (Read-Write) to File Server DR (Read-Only)
10 Gbps connection
NFS Volumes 20TB each.
File Server DR
A 100TB NAS Storage
Shared Namespace
- \\domainname\Share1
- \\domainname\Share2
- \\domainname\Share3
- \\domainname\Share4
- \\domainname\Share5

2.3.3. MariaDB Cluster

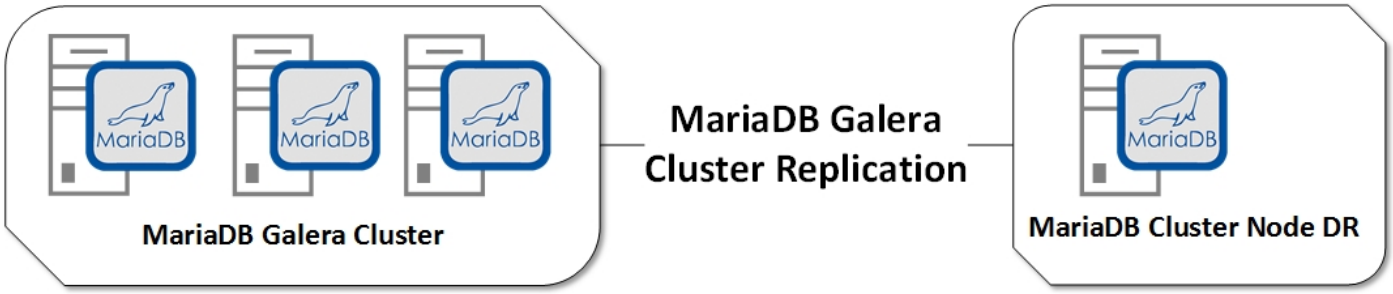
The MariaDB cluster is there and it is being used by our developers whom are fond of Open-Source projects, since we're using Galera Cluster we have the ability to add more nodes to our current cluster. In a master-master configuration, each node is able to accept writes and distribute them throughout the cluster.

In case the current cluster is being utilized as a Master-Slave the servers will need to have the patches known as "Galera" implement synchronous master-master replication.

At this point we have the 3 servers running behind a load-balancer (the Galera Load Balancer is a simple Load Balancer specifically designed for Galera Cluster) so we don't have to worry about the database server in the DR site being accessed by users or in other words we don't have to configure the DR site database node to be read-only because to the application it is invisible.

For the initial replication by default State Snapshot Transfer (SST) method is used, when a new node joins the cluster, the new node initiates a State Snapshot Transfer to synchronize its data with a node that is already part of the cluster.

After the initial replication has been performed, any new transaction that takes place on one of the nodes is committed then replicated to the whole cluster.



Monitoring of the Galera cluster can be done via CLI, but if more reporting is required a Cluster Control server must be installed and configured.

2.3.4. Other Services

So we still have our:

1- 15 Windows Servers holding various web applications (IIS and MSSQL).
2- 15 CoreOS Servers with Docker containers on them.
3- 2 Windows NT servers with IBM DB2 on them.

To address the protection of the up above servers we have chosen to utilize VMware Site Recovery Manager as a solution and we did not chose utilizing any kind of application availability for them.

Why not protection at the application level?

In terms of services 1 and 2 this is because we don't have any existing application clustering or availability implemented and if we are ought to implement availability at the application level it would

increase the complexity very much and the administration part will not be as much as agile and straight forward as we want it to be.

Now for number 3 this is a whole different story, we're in Mars and somehow people managed to get the 199x servers with them and sadly old applications and services get attached to their operating systems. Also Windows NT is a no longer supported operating system and most of the people whom are experts with Windows NT would not dare to tamper with these systems as long as they are running.

2.3.4.1. Required Components:

a. vCenter Server: The vCenter Server design includes a total of two virtual vCenter Server systems. One vCenter Server is located on Mars site and one vCenter Server on The Moon DR site. These are deployed within the management cluster at each site. Each vCenter Server provides management of the Cluster and integration with Site Recovery Manager.

b. Site Recovery Manager Server: This is required at both the primary site (Mars protected site) and the secondary site (The Moon recovery site). The Site Recovery Manager Server operates as an extension to the vCenter Server at a site.

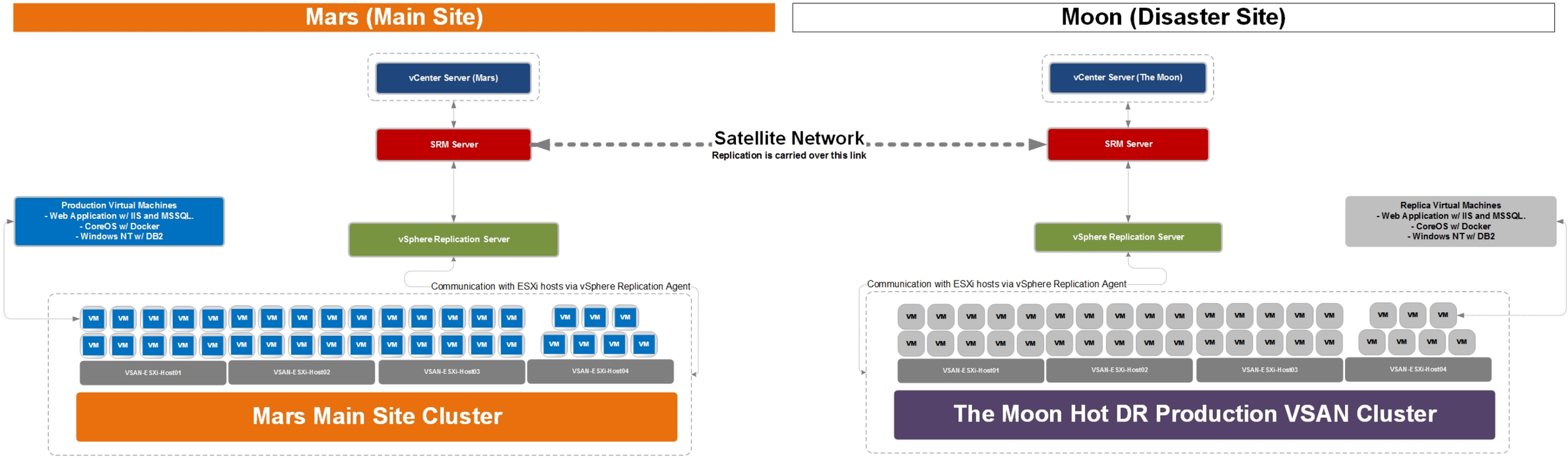
c. Site Recovery Manager Database: The Site Recovery Manager server requires its own database to store data, such as recovery plans and inventory information. The Site Recovery Manager database is a critical part of a Site Recovery Manager installation, and it cannot use the vCenter Server database because it has different database schema requirements.

d. A vSphere Replication Server: We will be utilizing vSphere Replication because we have VSAN utilized, vSphere Replication includes an agent built into vSphere and one or more virtual appliances that are deployed using vSphere Web Client. The agent tracks and sends changed data from a running virtual machine to a vSphere Replication appliance at a remote site; the appliance then adds the replicated data to the offline replica copy for that virtual machine. The vSphere Replication virtual appliance also manages and monitors the replication process.

e. Network configuration: Since we are going to use stretched VLANs in our design it is not necessary to change the IP addresses or any network configuration when recovering the virtual machines on The Moon recovery site.

After the initial full synchronization is complete, vSphere Replication will transfer only changed data. The vSphere kernel tracks unique writes to protected virtual machines, identifying and replicating only those blocks that have changed between replication cycles. This keeps network traffic to a minimum and allows for aggressive RPOs.

In addition, the virtual machine replication process is non-intrusive and takes place irrespective of the type of operating system or applications in the virtual machine. It is transparent to protected virtual machines and requires no changes to their configuration or ongoing management.


Mars (Main Site)
Moon (Disaster Site)
vCenter Server (Mars)
vCenter Server (The Moon)
SRM Server
Satellite Network
Replication is carried over this link
SRM Server
Production Virtual Machines
- Web Application w/ IIS and MSSQL.
- CoreOS w/ Docker
- Windows NT w/ DB2
vSphere Replication Server
vSphere Replication Server
Replica Virtual Machines
- Web Application w/ IIS and MSSQL.
- CoreOS w/ Docker
- Windows NT w/ DB2
Communication with ESXi hosts via vSphere Replication Agent
Communication with ESXi hosts via vSphere Replication Agent
VM
VSAN-ESXi-Host01
VSAN-ESXi-Host02
VSAN-ESXi-Host03
VSAN-ESXi-Host04
Mars Main Site Cluster
The Moon Hot DR Production VSAN Cluster

2.3.4.2. SRM Configuration Tables

- **Site Configuration**

Mappings	Protected Site (Mars)	Recovery Site (The Moon)
Resource	SRM Protection	SRM Recovery
Folder	Protected VMs	Recovery VMs
Network	VM-Network-VLAN101	VM-Network-VLAN101
Test Network	VM-Test-Network-VLAN201	VM-Network-VLAN201

- **Protection Groups**

PG Name	Description	Protected Site	PG Type
PG-1	Web Application Protection Group	Mars	vSphere Replication
PG-2	Docker Containers Protection Groups	Mars	vSphere Replication
PG-3	Windows NT Servers Protection Group	Masr	vSphere Replication

- **Recovery Plans**

Recovery Plan Name	Protection Group
RP-1	PG-1 - Web Application Protection Group
RP-2	PG2 - Docker Containers Protection Groups
RP-3	PG3 - Windows NT Servers Protection Group
RP-4	PG1, PG2 and PG3

The monitoring of Site Recovery Manager alarms is performed using the SMTP configuration of vCenter Server.

2.4. DR Site Backup

Well this is disaster site! Why would you need backup for it? As we mentioned before we are very paranoid with respect to disasters. Back on earth we have disaster sites till the point where we lost earth itself so DR sites were no longer something we can 100% rely on.

Since we are getting all the data from Mars and getting everything synchronized nicely we will have an enterprise class NAS storage connected to a single physical server where the backup software will be installed on it and where the NAS will host all the backups.

We are going to utilize **Symantec's Backup Exec** to backup only the data here, rather than doing the granular backups at the main site we will be doing it here for everything excluding:

1- Web Application VMs (these can be rebuilt or restored as VMs as they are static with no data).
2- CoreOS with Docker (these can be rebuilt as well).
3- Windows NT servers (sadly they don't have plugins for granular restore for that and they won't make one in the near future).

So we will be doing all the workloads that actually has valuable data that we can't compromise at all:

- Active Directory Database
- Exchange Mailboxes.
- Data on the file servers.
- MariaDB Database dumps (a script will run daily to export the databases, can be found in appendix D).

Backup schedule:

1- Full backups will take place at the end of each month.
2- Differential backups will take place each day.

Backup Retention:

1- The retention period will be 1 month for the full backup.
2- The retention period will be 1 week for the differential backups.

3. Disaster Site Validation

3.1. Active Directory Domain Services

For Active Directory Domain Service we can simply change the priority and weight of the domain controller then test if all services are pointing to the DR domain controller and that they're getting their authentication properly.

3.2. Exchange E-Mail Services

For the Exchange email services, we need to shutdown all Exchange Servers at the main site then activate the database copies on the DR Exchange server, finally using the DR OWA URL try to access the mailbox and attempt sending/receiving.

3.3. File Services

For the file servers, we actually don't have to do anything at all for testing in terms of reconfiguration. The DFS replicated folders can be accessed at any time and the files replicated can opened in read-only mode.

Should you want to test reverse the replication, the replication must be set to read-write then attempt to create/modify some files in DR and wait for the synchronization to complete.

3.4. Maria Databases

For the Maria databases, since we have a Galera cluster configured for multi-master and as mentioned before the load-balancer is pointing only to the nodes in the Main Site, we can put those nodes into maintenance/standby mode on the load-balancer then introduce the 4th DR node and then finally make a connection to the application from it.

3.5. Site Recovery Manager Replicas

For the SRM, we have a feature that will allow us to simulate the Recovery Plans that we have configured while using the test network which we have created.

If the VMs you're testing will require directory services to be properly tested you will need to clone the Active Directory server in the DR site (offline) and then change the clone's network to the test network before attempting to test the recovery plan.

3.6. Backup Validation

For the backup, you can perform restore at any time but it is preferable to attempt restoring items after each full backup has been processed successfully to insure the integrity of the backups.

4. Final Words

One can never get tired of protecting things that are precious to us, and as a human race we have learned that the hard and harsh, so at minimum its double to triple protection sometimes, RTO's and RPO's are important but eventually in extreme scenarios it's the data which is important.

For I used to work for a bank in my early days and the central bank required a DR plan for each bank, the requirement was simple the availability of the data must be 99.99999% and operability was merely mentioned. They only cared about guaranteeing the safety of the data.

5. Appendices

5.1. Appendix A – Exchange Server Monitoring Script

- http://exchangeserverpro.com/get-daghealth-ps1-database-availability-group-health-check-script/

5.2. Appendix B – DFS Replication Offline Seeding

- https://technet.microsoft.com/en-us/library/dn495052.aspx/

5.3. Appendix C – DFS Replication Monitoring Script

- http://community.spiceworks.com/scripts/show/1536-dfs-monitor-with-history

5.4. Appendix D – MariaDB Backup Script

- https://www.calmblue.net/blog/scripting/bash/mariadb-backup-database-script

5.5. Appendix A – References

- http://www.sqlservercentral.com/Forums/Topic1015210-1549-1.aspx
- http://www.sqlskills.com/blogs/paul/conference-questions-pot-pourri-4-how-many-databases-can-you-really-mirror-per-instance/
- http://www.militaryaerospace.com/articles/2012/06/laser-communications-feature.html
- http://www.slideshare.net/asertseminar/laser-communications-33264562
- http://www.space.com/1900-record-set-space-laser-communication.html
- http://www.continuitycentral.com/feature1137.html
- http://www.conceptdraw.com/solution-park/illustrations-aerospace-transport
- http://enterpriseit.co/microsoft-exchange/2013/dag-latency/
- http://enterpriseit.co/microsoft-exchange/2013/dag-dac-mode/
- http://blog.cirronix.com/2012/03/easy-sync-for-iis7-no-web-farm-required.html
- http://consulting.risualblogs.com/blog/2009/12/23/iis-how-to-tackle-multiple-web-servers-keep-them-in-sync/
- http://www.iis.net/learn/web-hosting/scenario-build-a-web-farm-with-iis-servers
- http://www.iis.net/learn/web-hosting/scenario-build-a-web-farm-with-iis-servers/planning-step-1-plan-iis-web-farm-infrastructure
- http://www.slideshare.net/MariaDB/mariadb-replication-state-of-the-art
- http://www.vmware.com/files/pdf/Exchange_2013_on_VMware_Availability_and_Recovery_Options.pdf
- http://www.slideshare.net/d0cent/orchestrating-docker-containersatscale
- http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2102453
- https://www.vmware.com/files/pdf/vsphere/VMware-vSphere-Replication-Overview.pdf
- https://technet.microsoft.com/en-us/library/cc730954.aspx
- https://technet.microsoft.com/en-us/library/dd979786%28v=exchg.150%29.aspx
- http://exchangeserverpro.com/exchange-server-2013-database-availability-groups/
- https://technet.microsoft.com/en-us/library/dd638104%28v=exchg.150%29.aspx
- http://blogs.vmware.com/vsphere/2011/10/srm-5-using-dependencies.html
- http://galeracluster.com/documentation-webpages/statetransfer.html

- https://mariadb.com/kb/en/mariadb/asynchronous-replication-with-galera-cluster/
- http://www.slideshare.net/skysql/mariadb-galera-cluster-simple-transparent-highly-available
- http://dba.stackexchange.com/questions/103997/galera-mariadb-and-multiple-datacenter
- https://groups.google.com/forum/#!topic/codership-team/K5Qm0BcLuM8
- https://mariadb.com/kb/en/mariadb/galera-load-balancer/
- http://www.fromdual.com/galera-load-balancer-documentation
- https://www.percona.com/files/presentations/percona-live/nyc-2012/PLNY12-galera-cluster-best-practices.pdf
- http://blogs.technet.com/b/askds/archive/2010/03/31/tuning-replication-performance-in-dfsr-especially-on-win2008-r2.aspx
- http://serverfault.com/questions/610917/one-dfs-replication-group-per-namespace
- http://blogs.technet.com/b/filecab/archive/2009/04/01/configuring-a-read-only-replicated-folder.aspx
- http://www.serverlab.ca/tutorials/windows/storage-file-systems/connect-windows-server-2012-r2-nfs-shares/
- https://technet.microsoft.com/en-us/library/cc772778%28v=ws.10%29.aspx
- http://social.technet.microsoft.com/wiki/contents/articles/438.dfs-replication-survival-guide.aspx
- https://www.digitalocean.com/community/tutorials/how-to-configure-a-galera-cluster-with-mariadb-on-ubuntu-12-04-servers
- https://www.linode.com/docs/databases/mariadb/clustering-with-mariadb-and-galera
- http://www.rackspace.com/blog/building-a-disaster-recovery-solution-using-site-recovery-manager-part-3-deploying/
- http://blog.scottlowe.org/2009/09/01/bc1500-site-recovery-manager-best-practices/