VIRTUAL DESIGN MASTER 3

IT'S ALL ABOUT THE (MOON) BASE DESIGN DOCUMENT V1.5

Challenge 3

Steven Viljoen
7-20-2015

Contents

Revision History

Date	Revision number	Author	Comments
16 July 2015	V1.0	S.Viljoen	Initial document draft
17 July 2015	v1.1	S.Viljoen	Business trip
17 July 2015	V1.2	S.Viljoen	Customer getting suspicious that all the typing is not related to taking in depth meeting notes.
18 July 2015	V1.3	S.Viljoen	Business trip – driving and typing is apparently frowned upon in some countries.
19 July 2015	V1.4	S.Viljoen	Seriously. How are you supposed to figure out reasonable RPOs and RTOs with no reasonable details?
20 July 2015	V1.5	S.Viljoen	Maria who?

Executive summary

Given the harsh environment on Mars and the importance of ensuring that key applications are able to be recovered in a disaster, we need to develop disaster recovery plans for the following applications.

1. Exchange servers
2. Web application servers
3. A 3 node MariaDB cluster
4. File servers
5. The Docker environment
6. Legacy NT4 servers running DB2

The moon has been chosen as a perfect offsite disaster recovery site and an advanced laser communication link has been built between Mars and the Moon bases for this purpose.

RPOs and RTOs should be defined for each application and a list of required software needs to be prepared.

Requirements

Reference	Description
RQ001	Provide offsite DRP for all key applications
RQ002	Define RPO and RTO for each application
RQ003	Minimize cross link laser bandwidth usage.
RQ004	Solutions must protect against logical corruption.
RQ005	

Constraints

Reference	Description
CS001	Laser link bandwidth is unknown.
CS002	Laser link stability is unknown.
CS003	

Risks

Reference	Description
RI001	No specific storage capacity is given to calculate backup times.
RI002	Application workloads are unknown.

Assumptions

Reference	Description
AS001	Einstein has been proven wrong about the speed of light. [1]
AS002	While only physical disaster scenarios have been discussed in the challenge it is assumed that logical corruptions need to be covered too.
AS003	The legacy NT4 servers have at least been virtualized using convertor 3.0.

[1] Advanced Laser Communication link provides 10ms latencies from Mars to Moon.

- Distance from Mars to Moon =224915600km
- Time taken (one way latency) for laser light to travel from mars to moon = 10ms
- Light in laser needs to travel at 80969472000000 km\h to achieve this.

Setting the stage…

<Enter stage left >

<Places head on chopping block>

HA is better than DR!

<Lifts head from chopping block>

<Aside> Sorry, but somebody needs to say it.

<To the audience>

Before we all lose our heads, let's take a closer look at what puts the 'disaster' in DR.

Physical disasters

These are the disasters that most people think about when planning for disaster recovery.

- Datacenter hit by meteor. (ok, maybe not one that is normally specifically planned for)
- Connectivity is taken out by solar storm.
- Mars destroyed to make way for an intergalactic highway off-ramp

When it comes to Physical disasters, a multisite HA solution is in many ways better than a disaster recovery process as it provides an immediate secondary avenue for data\traffic flow without the wait for failovers to complete or standby servers to be spun up.

Logical disasters

These are more common yet less likely to be planned for.

- System administrator runs DROP TABLE on the master.
- A buggy MS patch takes down the whole windows environment

Logical disasters really only have 1 solution. Backups.

Any DR solution that uses replication (SRM for instance) does nothing more than replicate the issues to the other sites. This is true for both synchronous and asynchronous replication. Asynchronous replication theoretically can get around this by setting the sync interval with enough delay to allow for an administrator to a) identify that some type of logical corruption has occurred and b) stop the replication before the corruption is propagated.

HA solutions in some cases can overcome logical corruptions (Windows cluster protecting against a bad MS patch on 1 node), but are also not always immune.

Backups

The ultimate time machine. Allowing us to undo all evils that cross our daily admin path.

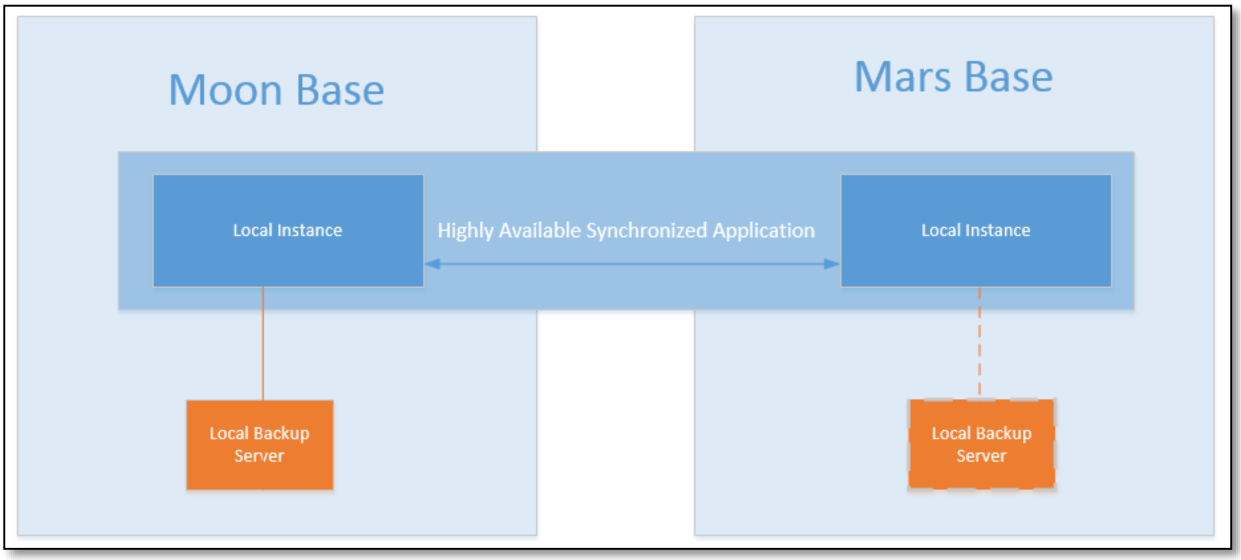
However, for backups to be useful they need to be stored offsite and that is where the problems begin, especially if you have a state of the art laser communication link and all you know about it is that it breaks the known laws of Physics[AS001] and has a 10ms latency.

Conceptual Design

To ‘make sure that we are planning for every contingency’ we need a DR solution that covers both physical and logical disasters and at the same time does not make use of critical assumptions such as available bandwidth, link stability or storage device types.

The solution I have chosen for this challenge is as follows.

- Increase HA of the applications by stretching them across Moon and Mars sites.
  - This covers all physical disasters on Mars.
  - Provides continuous availability in case of physical disaster.
- Run backups on the DR site instances.
  - Provides protection against logical corruption.
  - Provides offsite (from Mars perspective) backups
    - without impacting the production load on Mars
    - without consuming the laser link bandwidth by moving backups across the link



Onsite backups

As shown in the diagram below it is possible to extend the backup solution to the protected site (backups will remain onsite) to allow for quick local restores if needed and possible.

It is also possible to stagger the local and DR site backups to provide shorter RPOs while using the same amount of storage and taking the same amount of time.

Backup site	Data set	Time started	Backup size
Moon	Exchange database A	12:00 daily	500 GB
Mars	Exchange database A	12:00 daily	500 GB

The RPO of Exchange database A is 24 hours using either the Moon or Mars backup.

Backup site	Data set	Time started	RPO
Moon	Exchange database A	12:00 daily	500 GB
Mars	Exchange database A	00:00 daily	500 GB

In the latter table Exchange database A can be restored using either the Moon or Mars backup which are taken 12 hours apart on different sides. Thus the same space is consumed but the RPO for Exchange dataset A has dropped to 12 hours.

Common Infrastructure services

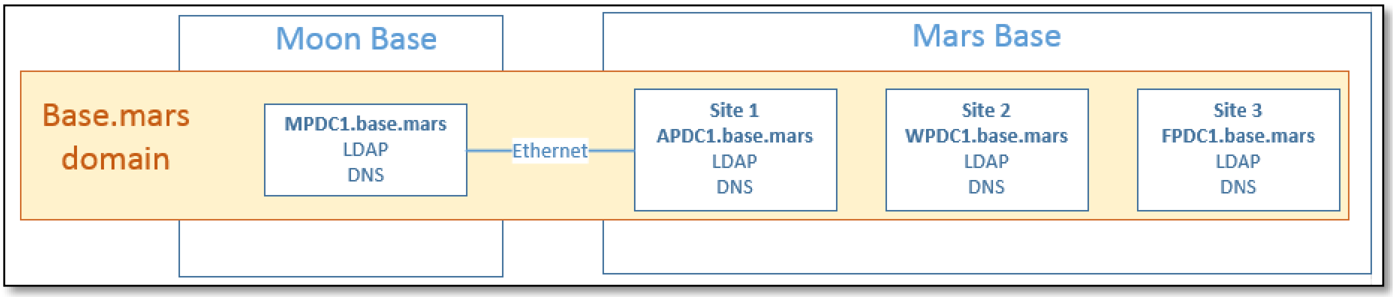
The following common infrastructure services will be required on both the Protected site as well as on the Recovery site.

- LDAP services
- DNS services
- Time Synchronization
- DHCP services

LDAP\DNS

The existing 'base.mars' domain infrastructure on Mars will be extended by adding an additional Domain Controller on the moon to provide LDAP and DNS services for the 'base.mars' domain at the DR site.

All will be configured as Global Catalogue Servers.

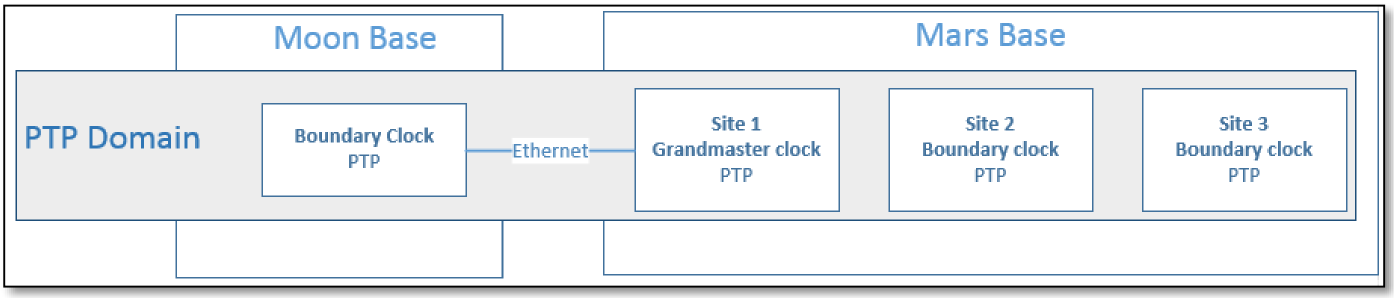


The benefits of this setup.

- Provides a HA option that covers:
  - Entire Datacenter failures on Mars
  - Connectivity failures between Mars LDAP servers and Mars Clients
- Allows for offsite backups to be made locally on the moon site without the need for replicating the backups across the laser link as would be the case if the domain backups were made on the Mars site. [RQ003]

Time Synchronization

The existing PTP domain infrastructure will be extended across to the moon base by adding an additional boundary clock on the moon site. This will allow for highly accurate time synchronization across both environments.



While the diagram shows the Grandmaster clock being located in Site1 on Mars it is purely to show the high level component layout. In reality the grandmaster clock will be automatically selected according to the best master clock (BMC) algorithm and could therefore be located at any of the four sites.

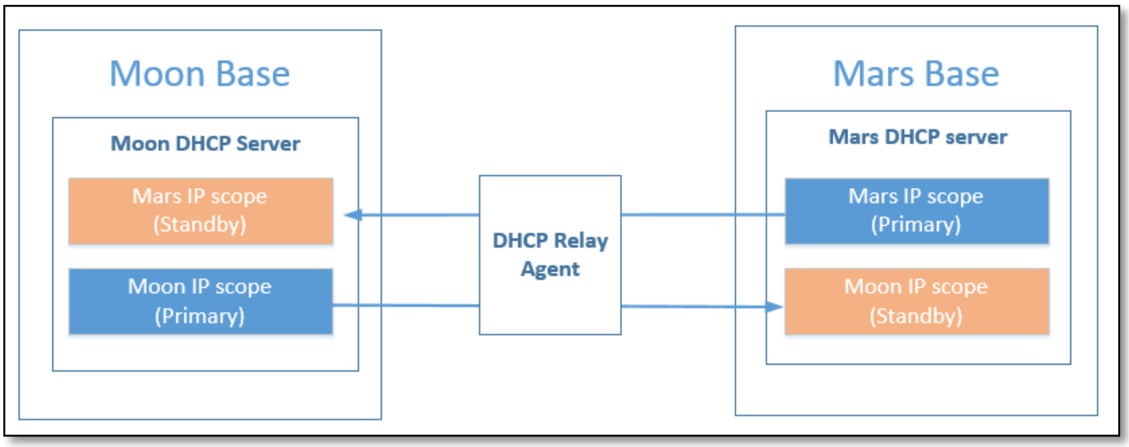
DHCP

An important but often overlooked aspect to any Disaster Recovery environment is the need for a DHCP server at the recovery site. Without this, users on Mars will not be able to receive IPs or renew their IPs while the Mars based DHCP servers are down and thereby nullifying the point of any DR solution.

(This is assuming of course that Mars is not running some kind of employment creation project under which the Chief static IP assigner and his colleague Chief static IP trouble-shooter are responsible for ensuring that all client computers are manually assigned static IPs).

To ensure this 2 DHCP servers will be deployed (1 primary on Mars and 1 standby on the Moon) using the new WS2012 DHCP hot standby mode. During normal operations the Mars DHCP server will provide IP addresses and other NW configuration to the Mars users, however in the event that the Mars DHCP server is down the Moon DHCP server will continue to provide the service to the users on Mars.

The additional advantage of this is the ability to use the same two DHCP servers to provide DR for both the Mars and the Moon base by assigning two different scopes protected by two failover relationships as shown below.



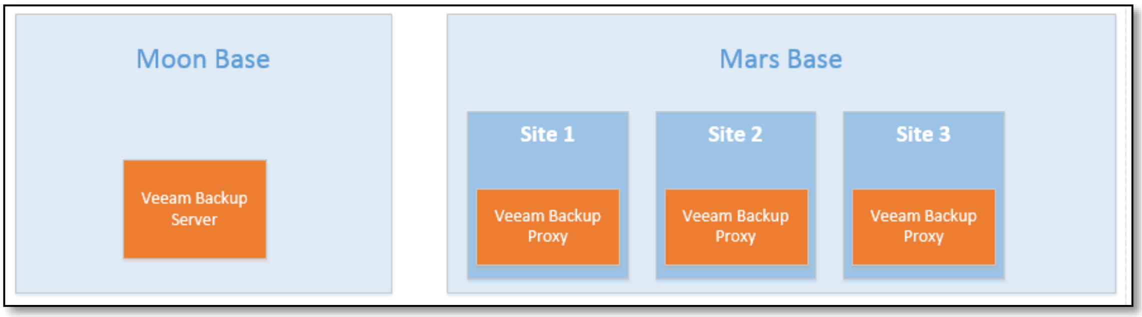
Backup Infrastructure

For the backup solution I will be using Veeam 8 Backup and replication.

The benefits of Veeam backups are:

- It is agentless and storage agnostic.
- Provides instant VM recovery
- Provides instant file-level recovery
- Built-in, source-side compression & deduplication

The Veeam Backup server will be located on the Moon site with 1 Veeam backup proxy located in each Mars site to provide for local backups. This provides a single pane of glass views of all backups across all sites.



Specific backup schedules are documented in each application section below.

Application servers

Exchange servers

Design choice

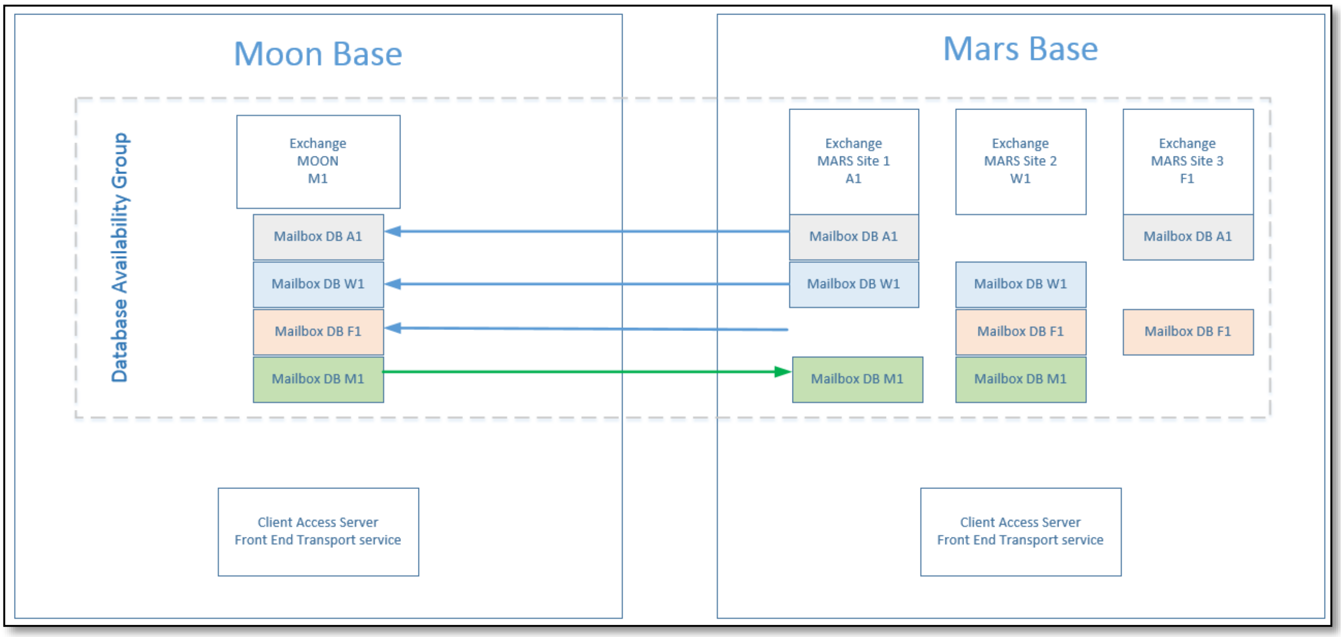
The exchange servers will be protected by using MS Exchange 2013, adding an additional mailbox at the Moon site and creating a multisite Database Availability Group (DAG) that is spread across the Moon and 3 Mars sites.

The benefits of this are:

- Multiple levels of site resiliency are created. (Locally across 3 Mars sites + offsite to Moon)
- Mail routing is handled by the mailbox members based on the Routable DAG rather than relying on Active directory Sites.
- No shared storage is needed.
- Full mailbox database replicas are created and hosted on various mailbox servers across sites.
- Highly scalable solution. Adding a new site involves 'simply' adding the new mailbox server to the DAG.
- Offsite backups can be made locally on the Moon site.
- Able to provide a DR solution for the Moon site with only a small amount of additional configuration.

Design

The exchange layout is shown in the diagram below.



Each mailbox database will have an additional copy in at least 2 separate sites, one of which will be the mailbox server located on the Moon site. This will provide local site resiliency for Mars and DR resiliency on the Moon site.

RPOs and RTOs

The exchange infrastructure is considered non-critical in the Mars environment. This together with the Multisite HA solution means that a 24 hour RPO should suffice. [RI002]

Disaster type	RPO	RTO
Physical disaster	**<5 min** A small amount of un-replicated data could still be in the ESE buffer when the failure occurs.	**0 Min** Mailbox database is still available on the moon site and possibly on 1 additional mars site.
Logical disaster	**<24 hours** Daily incremental: Every day: 18:00 Synthetic full: Every Saturday 21:00	**< 1 hour** Using Veeam Instant VM recovery.

MariaDB cluster

Design choices

The MariaDB cluster will be protected by migrating it to a Galera cluster (if needed) and then adding a fourth node on the DR site (Moon).

The benefits of using Galera include:

- Easy migration to Galera cluster
- Uses a quorum model to prevent portioned nodes committing transactions.
- Multi-master setup
    - Read and write operations can be directed to any node.
- Automatic node provisioning
- Synchronous data buffer replication ensures crash consistent state across all nodes.
- Possible to mix replication methods
    - Setup an async slave (time delayed sync).

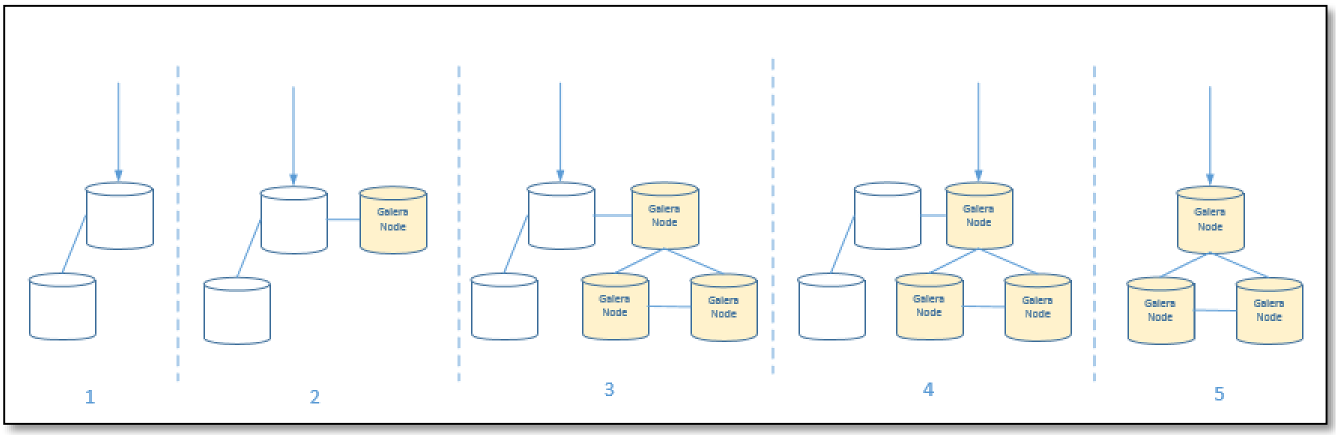
Synchronous buffer replication

1. Transactions are processed on local server until *COMMIT* command from client.
2. Transaction is then replicated to all nodes in cluster.
3. Client receives OK status
4. Transaction is applied in slaves.

Migrating to a Galera cluster

Assuming that the current MariaDB environment is not running Galera it is a very simple operation to migrate.

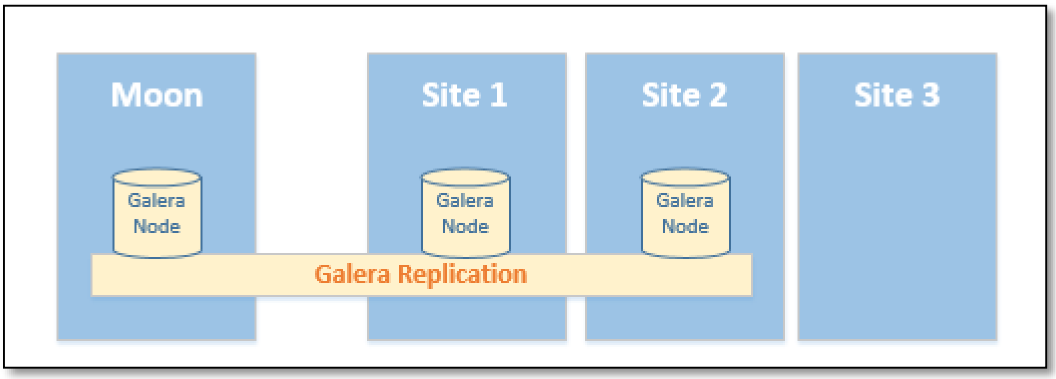
1. Start with regular setup
2. Add a Galera node as a normal slave.
3. Join additional nodes in the Galera slave cluster.
4. Direct traffic to the Galera cluster.
5. Remove the original non-Galera servers.



Design

As Galera uses a quorum model it is needed to have an odd number of nodes.

Rather than adding 2 additional nodes at the moon base (5 total) this design will replace one of the existing Mars based nodes with a moon based node as shown below.



The 3rd node on Mars can be used as a dedicated donor node for the new Moon node initial synchronization.

Adding the additional Moon node.

1. Install\Configure the Moon node.
2. Remove the 3rd Mars node from the cluster.
    a. This will prevent any impact to the remaining cluster nodes during the initial state transfer.
3. Connect Moon node to 3rd Mars node for the initial State Snapshot Transfer (SST).
4. Once completed add the Moon node to the existing cluster and allow automatic donor selection for the Incremental State Transfer (IST).

This approach still provides multiple levels of resiliency (Across Mars sites + Moon\Mars) while keeping the solution as simple as possible. It also allows for offsite backups to be made locally on the moon site without impact to either the production site (Mars) or cross site link bandwidth.

RPOs and RTOs

As this is apparently the only DB cluster running on Mars it is assumed that it is used by a number of applications and therefore has a high data change rate. [RI002]

Due to this the RPO will be defined as 6 hours to avoid too much data being lost but still allow large backups to complete. [RI001]

Disaster type	RPO	RTO
Physical disaster	**0 min** Crash consistent	**0 Min** Database is still available on the moon site and possibly on 1 additional mars site.
Logical disaster	**<6 hours** Veeam backup is set as follows: Daily incremental: Every 6 hours Synthetic full: Every Night 21:00	**< 2 hours** (Based on similar system setups) Using Veeam Instant VM recovery.

File Servers

Design choice

DFSR will be used to protect the 5 file servers for the following reasons:

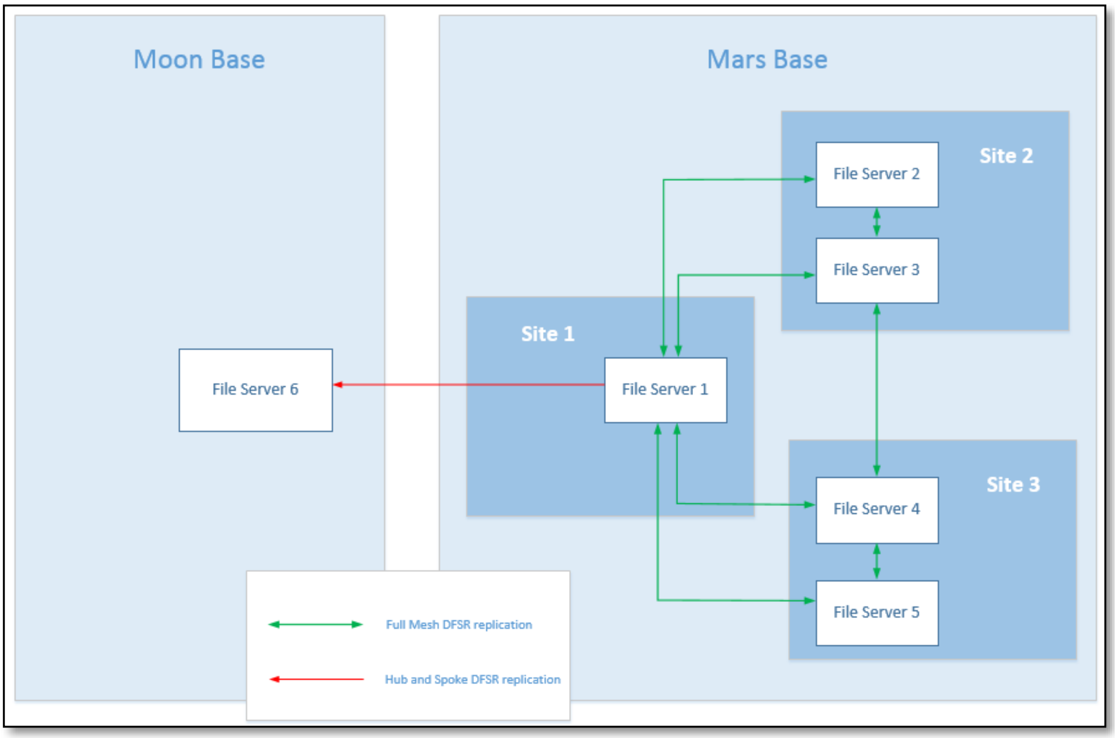
- DFSR is designed for replicating data across slow WAN links.
    - Remote differential compression (RDC) helps reduce the amount of network bandwidth used for replication.
    - DFS Replication can resume replicating any partially replicated files that result from WAN interruptions.
    - Cross-file RDC can be used to identify files that are similar to the file that needs to be replicated. Instead of replicating the entire file, DFS Replication can use portions of files that are similar to the replicating file to minimize amount of data transferred over the WAN.
- Replication can be scheduled to occur during off-hours.
- Bandwidth throttling can be set to regulate how much bandwidth is used during replication.

To further reduce the cross link bandwidth usage and initial sync time the design will make use:

- Preseeding of the data files from File Server 1 to File Server 6 once the full mesh data sync has completed.
- Cloning the DFSR database from File Server 1 to File Server 6 once the full mesh data sync has completed.

Design

The custom DFSR replication topology is shown below.



Mars site

On the Mars side the 5 existing File servers will be distributed across sites in a Full Mesh DFSR replication topology.

No information is provided as to the current structure and use of the file servers but it is assumed that they are 5 standalone file servers (no redundancy built in) so this design will use 5 separate Namespaces (1 primary per server) to ensure that information added to any will be replicated to all others. This will ensure information consistency across all 3 sites on Mars in case the various 3 sites are cut off from each other.

This does come at an increased storage capacity cost but the assumption is that not every server will be fully utilised and it also prevents possible homicides when crazy cat lady goes on a rampage as she is not able to upload the latest photos of her cat, Felicette, enjoying the Martian microgravity.

DFSR replication for the full Mesh topology does not affect the Laser Link bandwidth [RQ003] and as such will be set to continuous replication.

Moon DR Site

An additional (hub-spoke) DFSR replication topology will be set up between File Server 1 on Mars and the new Moon file server 6.

This will be set to replicate after office hours only to minimize bandwidth impact.

Daily replication: Every day 18:00 – 06:00

The benefits of this configuration are:

- File Server 6 (Moon) will contain all data spread across the 5 Mars file servers.
- Offsite backups could be taken locally of File Server 6 without additional impact to the cross link bandwidth.
- Bidirectional replication could potentially be setup in the future which would allow Moon data to be replicated and spread across the 5 Mars file servers.

RPOs and RTOs

Given that this will mostly be used for personal storage (cats and dog pictures) and the rate of data change is not expected to be very high based on the anticipated population on mars the RPO is set at 24 hours. [RI002]

As the replication from file Server 1 (Mars) to File Server 6 (Moon) takes place every 12 hours the backups will be scheduled to run after this window. While this is business hours it is the passive node and as such will not be any impact for users.

Disaster type	RPO	RTO
Physical disaster	**<16 hours** DFSR replication scheduled to run every 12 hours with anticipated sync time of 4 hours.	**0 Min** File server is still available on the moon site and possibly on 1 additional mars site.
Logical disaster	**<24 hours** Veeam backup is set as follows: Daily incremental: Every day: 10:00 Synthetic full: Every Saturday 11:00	**< 5 hours** (Based on similar system sizing) Using Veeam Instant VM recovery.

Web application servers

Design Choice

To protect the web application servers the local SQL databases on each will be consolidated to a 2 node SQL AlwaysON cluster with 1 node located on the Moon site and 1 node on the Mars site.

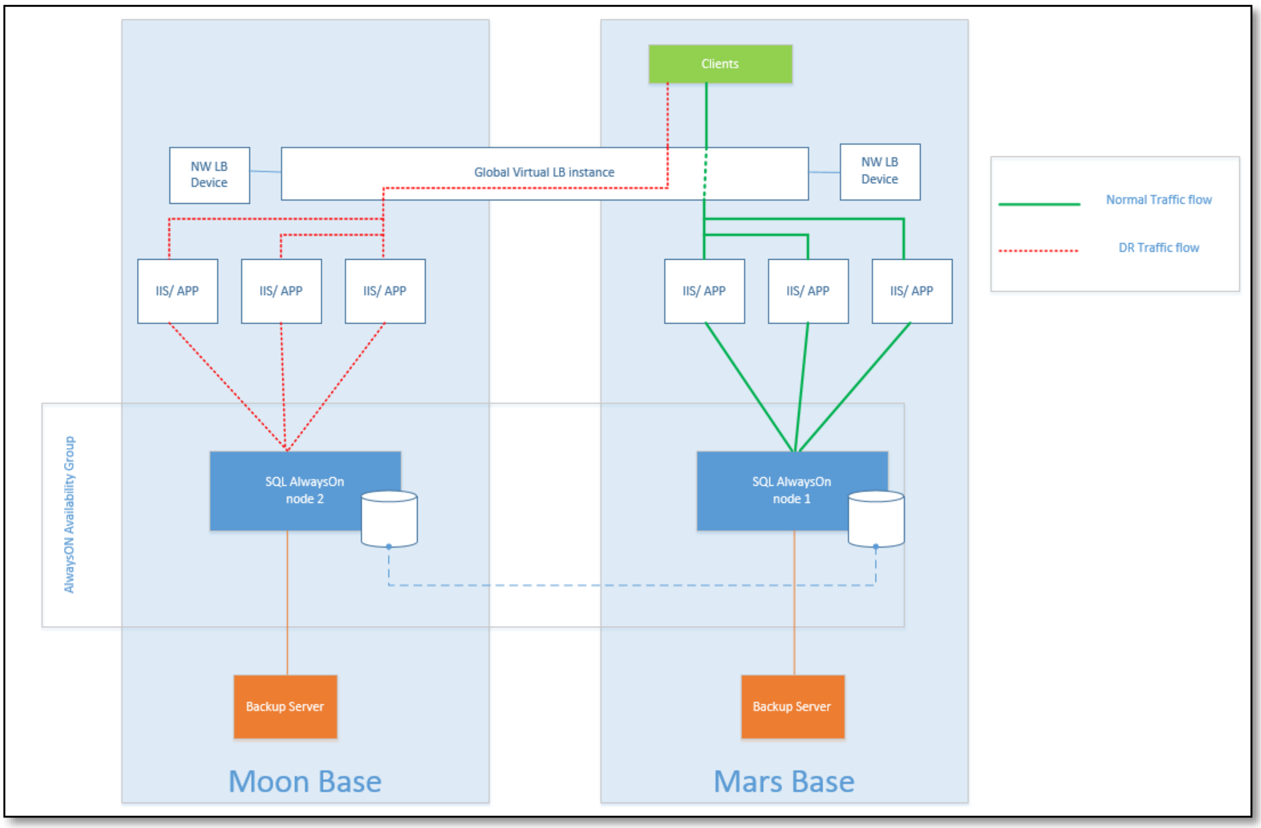
The IIS servers will reside on both Sites and a Global Load Balancer (GLB) consisting of 2 NW load balancers (1 per site) and a Virtual LB instance will be deployed across both sites.

For normal operation the GLB will direct local traffic to the local IIS servers, however in case of a site failure on Mars traffic will be directed to the DR sites environment.

This design can easily be configured to provide a similar service to Moon residents.

Design

The environment layout is shown below.



RPOs and RTOs

As there is not much ecommerce anticipated on Mars it is assumed that these web application servers will mostly be used for time tracking and inventory type applications. [RI002] They are designated as non-critical systems with a 24 hour RPO.

Disaster type	RPO	RTO
Physical disaster	**<30 min** Based on SQL AlwaysON replication and the static nature of IIS configurations.	**5 Min** Web servers will still be accessible on the Moon site. 5 min is based on 300sec connection draining configuration on the GLB.
Logical disaster	**<24 hours** Veeam backup is set as follows: Daily incremental: Every day: 20:00 Synthetic full: Every Saturday 20:00	**< 2 hours** Based on estimated time to recover biggest component (DB). Using Veeam Instant VM recovery.

CoreOs\Docker servers

Design choices

To protect the Docker servers this design will be using OpenSVC with dds replication.

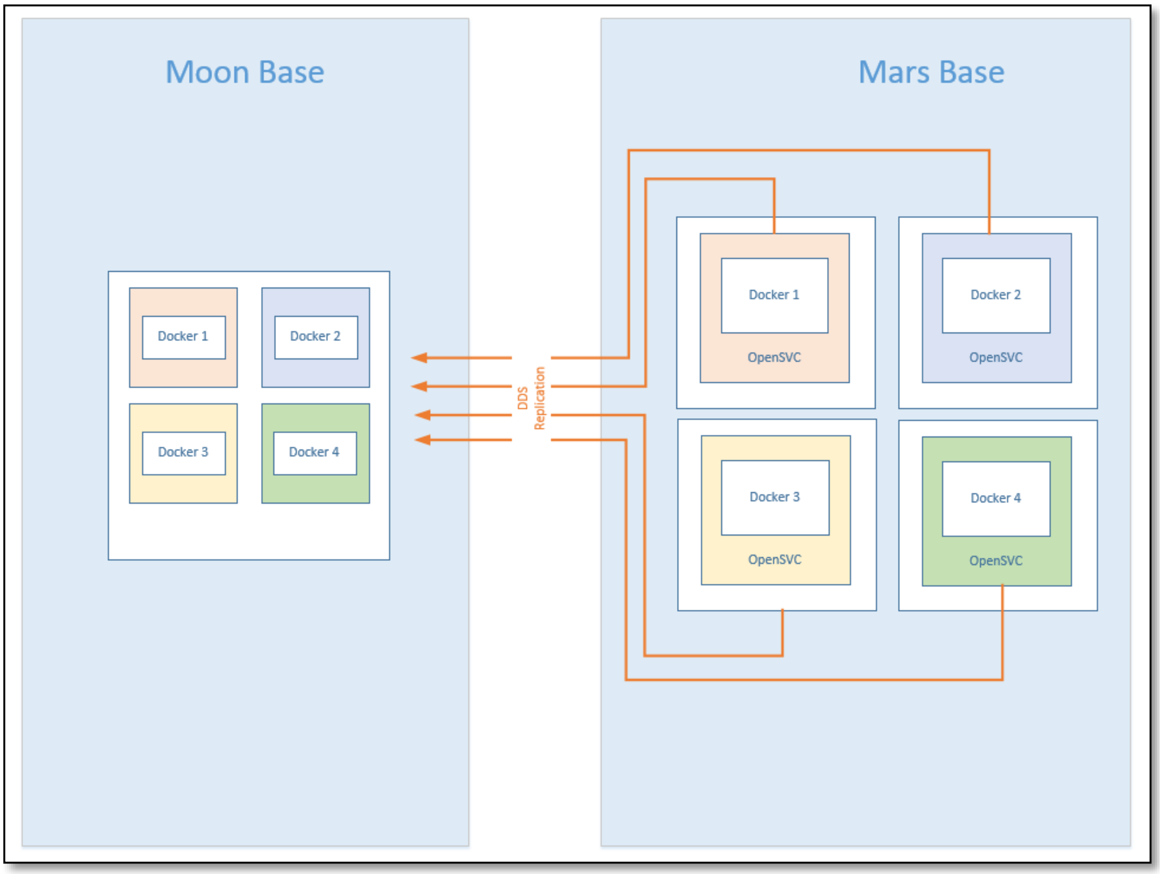
The benefits of using this combination are:

- Provides a common set of start, stop and status commands across different operating systems.
- Scoping deals with server differences between source and target by allowing resource parameters to be changed based on context.
- Supports multiple replication modes.
- Highly scalable and simple setup.
- Has minimal dependencies.
- Very modular data replication setup
- DDS replication is IP based.

Given the modular replication setup the OpenSVC services will be consolidated on the DR site to run on 1 virtual machine. This will reduce RTO time as it allows all services to be controlled jointly via single commands rather than needing to control each individually (i.e. using one command to start all services on the DR site rather than needing to start each service individually).

Design

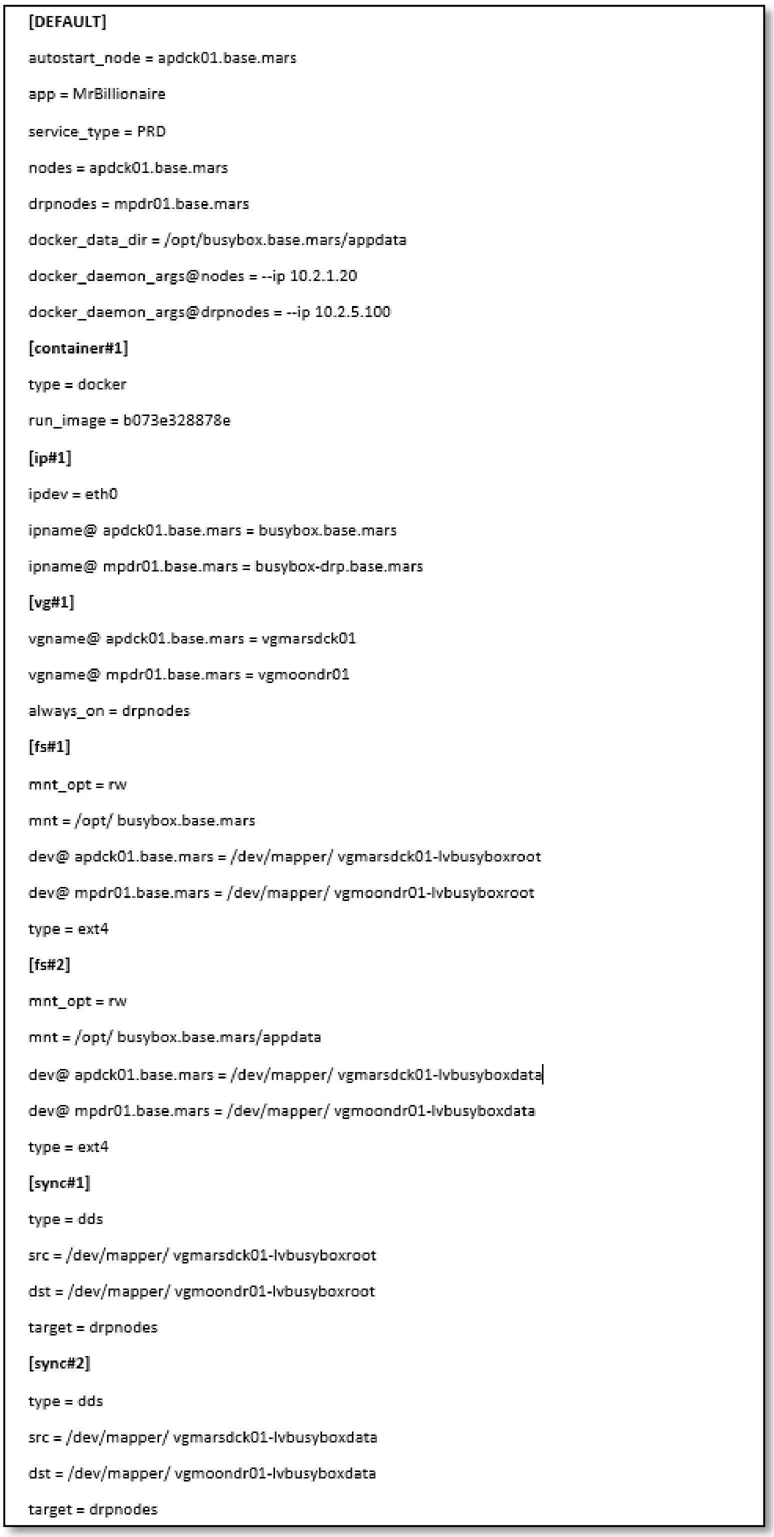
The DR layout is shown below. For brevity only 4 instances have been shown but as mentioned above all instances will failover to a single system on the moon site.



This approach also simplifies the backup of the DR site as there is only 1 server to backup and allows for offsite backups to be made locally on the Moon site.

Configuration setup example

The following section shows the configuration file setup on a single protected server.



```
[DEFAULT]
autostart_node = apdck01.base.mars
app = MrBillionaire
service_type = PRD
nodes = apdck01.base.mars
drpnodes = mpdr01.base.mars
docker_data_dir = /opt/busybox.base.mars/appdata
docker_daemon_args@nodes = --ip 10.2.1.20
docker_daemon_args@drpnodes = --ip 10.2.5.100
[container#1]
type = docker
run_image = b073e328878e
[ip#1]
ipdev = eth0
ipname@ apdck01.base.mars = busybox.base.mars
ipname@ mpdr01.base.mars = busybox-drp.base.mars
[vg#1]
vgname@ apdck01.base.mars = vgmarsdck01
vgname@ mpdr01.base.mars = vgmoondr01
always_on = drpnodes
[fs#1]
mnt_opt = rw
mnt = /opt/ busybox.base.mars
dev@ apdck01.base.mars = /dev/mapper/ vgmarsdck01-lvbusyboxroot
dev@ mpdr01.base.mars = /dev/mapper/ vgmoondr01-lvbusyboxroot
type = ext4
[fs#2]
mnt_opt = rw
mnt = /opt/ busybox.base.mars/appdata
dev@ apdck01.base.mars = /dev/mapper/ vgmarsdck01-lvbusyboxdata
dev@ mpdr01.base.mars = /dev/mapper/ vgmoondr01-lvbusyboxdata
type = ext4
[sync#1]
type = dds
src = /dev/mapper/ vgmarsdck01-lvbusyboxroot
dst = /dev/mapper/ vgmoondr01-lvbusyboxroot
target = drpnodes
[sync#2]
type = dds
src = /dev/mapper/ vgmarsdck01-lvbusyboxdata
dst = /dev/mapper/ vgmoondr01-lvbusyboxdata
target = drpnodes
```

Replication settings

(Units are in minutes)

sync_min_delay = 20	/Minimum time before a new sync can be triggered.
sync_interval = 40	/Regular sync interval.
sync_max_delay= 60	/Max time after which sync is considered 'stale'

Configuration overview

The high level steps to protecting the Docker infrastructure are as follows:

1. Configure the source service.
2. Declare the target server as a DRP node. / drpnodes = xxxx
3. Configure scoping to deal with server differences
   a. Docker parameters / docker_daemon_args
   b. IP addresses / [ip#1]
   c. Volume groups / [vg#1]
   d. Logical volumes / [fs#1], [fs#2]
4. Configure replication. / [sync#1],[sync#2]
5. Trigger an initial full data sync.

RPOs and RTOs

Given that these are the only application based servers mentioned it is assumed that they are critical. [RI002]

Restore RPO is defined as 6 hours.

Disaster type	RPO	RTO
Physical disaster	**<80 min** Based on sync_max_delay setting and estimated sync time.	**30 Min** Estimated time required to start all services on the consolidated Moon server.
Logical disaster	**<6 hours** Veeam backup is set as follows: Daily incremental: Every 6 hours. Synthetic full: Every Night: 00:00	**< 2 hours** Based on estimated size. Using Veeam Instant VM recovery.

Legacy NT4 servers

Seriously?

I am assuming that it was the sysadmin supporting these 2 dinosaurs that 'accidentally' left the datacentre door open during the dust storm in the first place.

Design Choices

Given the temperamental nature of the underlying OS the best solution would be to preserve as much of the functional (and I use that term very lightly) bundle as possible. The DR solution should encapsulate the entire VM [AS003] and move it to the DR site with as little delay as possible.

For these reasons I have decided to go with a simple hypervisor based Zerto replication to the moon site.

The benefits of using this solution are:

- Storage agnostic.
- Can be replicated to an AWS type cloud if needed.
- Zerto provides RPOs in seconds with WAN bandwidth optimization.
- Journaling allows the recovered server to be brought up to any point in time within the last 5 days.
- Offsite backups are executed at the recovery site (Moon site) so there is no impact to the production sites.
- Backup packages contain VM information + metadata so they can be recovered to different sites.

Design

Both NT4 servers will be protected by Zerto and replicated across to the DR site.

RPOs and RTOs

These are either non-critical servers given that they run DB2 on an archaic Operating system or are extremely important and there has never been a downtime to upgrade to a newer OS.

Either way, using Zerto, the expected RPO is 1 hour.

Disaster type	RPO	RTO
Physical disaster	**< 1 hour** No multisite HA option	**< 2 hours** (Anyone that has worked with NT4 will know why it takes so long to start\reboot\reboot again)
Logical disaster	**<1 hour** Using Zerto journal	**< 2 hours** See above.

Backups will not be used for the NT4 servers as Zerto journaling provides a 5 day Point in Time recovery option.If a longer retention time is needed then manual checkpoints can be created.

The elephant in the room

Why was Zerto not used for all applications if it provides replication (physical disaster protection) + Point in Time journaling (logical disaster protection)?

The reasons:

- Zerto does not extend the HA of an application meaning that it is impossible to get a 0min RTO.
- Extending the HA of an application across to the moon site can in most case provide valuable infrastructure for the poor forgotten colony on the moon.
- Size does matter. Especially when we are talking about replicating all applications across an unknown bandwidth of unknown stability [CS001], [CS002].

References

MariaDB.com. "Getting Started with MariaDB Galera Cluster." n.d. <https://mariadb.com/kb/en/mariadb/getting-started-with-mariadb-galera-cluster/#server-configuration-limits>.

—. "How to Understand Galera Replication." n.d. <https://www.percona.com/live/mysql-conference-2013/sessions/how-understand-galera-replication-0>.

Microsoft. *Planning for high availability and site resilience*. 05 08 2014. <https://technet.microsoft.com/en-us/library/dd638104(v=exchg.150).aspx>.

Mota, Nuno. *Exchange 2013 Mail Flow (Part 1)*. 29 11 2012. <http://www.msexchange.org/articles-tutorials/exchange-server-2013/planning-architecture/exchange-2013-mail-flow-part1.html>.

OpenSVC.com. "Service configuration file template." n.d. <https://docs.opensvc.com/agent.template.env.html>.

—. "Supported data replication modes." n.d. <https://docs.opensvc.com/agent.feature.matrix.html>.

Pyle, Ned. *DFS Replication Initial Sync in Windows Server 2012 R2: Attack of the Clones*. 2013. <http://blogs.technet.com/b/filecab/archive/2013/08/21/dfs-replication-initial-sync-in-windows-server-2012-r2-attack-of-the-clones.aspx>.