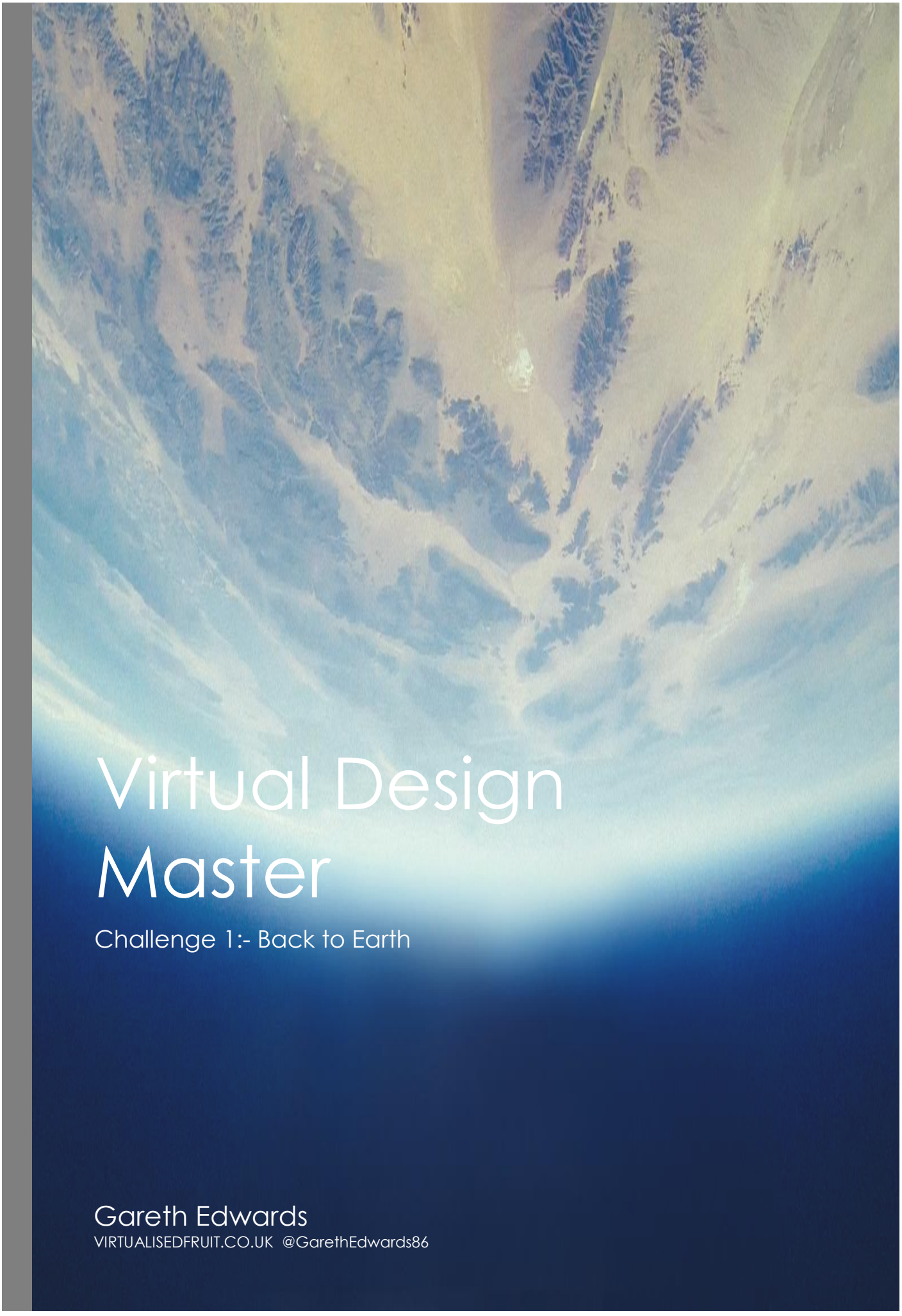


Virtual Design Master

Challenge 1:- Back to Earth

Gareth Edwards
VIRTUALISEDFRUIT.CO.UK @GarethEdwards86

Cover from (Pexels, n.d.)

[Synopsis]

We've had quite a journey so far during the first three seasons of Virtual Design Master. We've had to survive the zombie apocalypse and evacuate our planet. We've needed to support human life on the moon and Mars, and now, we're going back to earth.

We ended last season by giving the zombies a taste of their own medicine. Thanks to Steven, last season's Virtual Design Master, the zombie anti-virus was applied by the Zombie Assassin System. Over the last year, we've monitored the zombies closely and it seems most of them no longer exist.

It is time to take back our planet, but before we can, we need an infrastructure to support re-colinization. Does everyone remember the warehouse of 5 year old hardware from Season 1? Unfortunately it isn't usable any more.

Luckily our billionaire friend has been recruiting to re-build his empire, and his first order of business is datacenter hardware. Since we're starting from the ground up, you can use any type of hardware you would like, even if it doesn't exist yet. While the sky is the limit, remember to justify your hardware decisions.

Unfortunately, we are still limited by software. You can use any cloud software suite you would like that exists today, and you can assume it will run on the new hardware. Prepare a multi site environment for the world's new infrastructure. Your primary site is on Earth, wherever you would like it, and your secondary site is on the moon. The most critical application is the HumanityLink software suite, which consists of three front end web servers, one database, and two application servers. Performance of this software is paramount. The environment must also support 25 web servers, 5 databases, and 10 application servers.

Table of Contents

1) Executive Summary

a) Project Overview

The zombies are gone or so we think and this project is all about building a resilient infrastructure so we can rebuild earth and the human race.

b) Intended Audience

This guide is intended for the vDM judges and any one left to help rebuild the human race.

c) Project Summary

This project was the skies the limit style project of which never happens in real life as our billionaire friend wants the human race to survive. We have very limited requirements and no constraints with what appears to be an endless budget. Maybe this project is to lead the vDM challenge candidates into a false sense of security as there is a distinct lack of evilness before the next challenge.

i) Project Requirements

PRQ001. We must provide two sites, one on earth and one on the moon

PRQ002. The system must support the HumanityLink software suite, which consists of three front end web servers, one database, and two application servers. Performance of this software is paramount. The environment must also support 25 web servers, 5 databases, and 10 application servers.

ii) Project Assumptions

A001. The old warehouse is no longer and we can go on a shopping spree
A002. We are able within reason and without trying to break the laws of physics set some abstract figures to hardware that may have advanced from todays
A003. Our billionaire friend is going to want to prepare for the next outbreak just in case
A004. There may be zombies still hiding out there
A005. This risk of airborne infection is now low
A006. There are no issues with power
A007. There are no issues with cooling
A008. There are no issues with space
A009. Our billionaire friend will also want to own and provide a worldwide mobile telephony company that provides 99/100% worldwide coverage but maintained by another arm/team
A010. The satellite uplink will not get affected by any atmosphere changes or issues and be 100% reliable
A011. The HumanityLink software suite is deemed as business critical and not life as this has not been established within the scope provided
A012. We may have another site or lab we can use if really required in event of another disaster
A013. All current cloud services by vendors are still available to use
A014. All IT personnel have access to a detailed and update to date CMDB at all times
A015. Although we are limited to major site we can have access to multiple satellite station uplinks
A016. Our billionaire friend hasn't set a budget
A017. Speedy transatlantic fibres still exist
A018. The critical user data we need to replicate of which must be always available is less than 1TB
A019. The databases that have been requested are no more than 1TB in size
A020. We have access to an email platform
A021. The application will be accessed via a webpage much like Twitter, Facebook, Google etc

iii) Project Constraints

C001. We will still be limited by the laws of physics but we have been provided none

iv) Project Risks

PRI001. The atmosphere on earth is still not yet understood so may not always be inhabitable
PRI002. Software can still break but this is mitigated by having the best developers on hand to diagnose the software
PRI003. We end up making AI that wants to harm us anyway!

2) Design Summary

a) Physical Design Overview

For the purpose of building our new infrastructure we have selected some items for ease of management with the feature set that they provide. We need to focus on all levels of the datacentre to its physical location, hardware used and software layers. Where possible we want to have some agnostic features into the system such as storage so if down the line we find better systems are available we can easily swap out our current components. Where possible we will also try to provide multiple layers of resiliency, the cost of this may well carry additional vendors to learn but the systems must always be operational where possible. I don't think we should mind as we have the best of breed engineers on this build. This is usually not possible as costs are a constraint but in this case our billionaire friend appears to have provided a blank cheque as he wants humanity to survive and thrive.

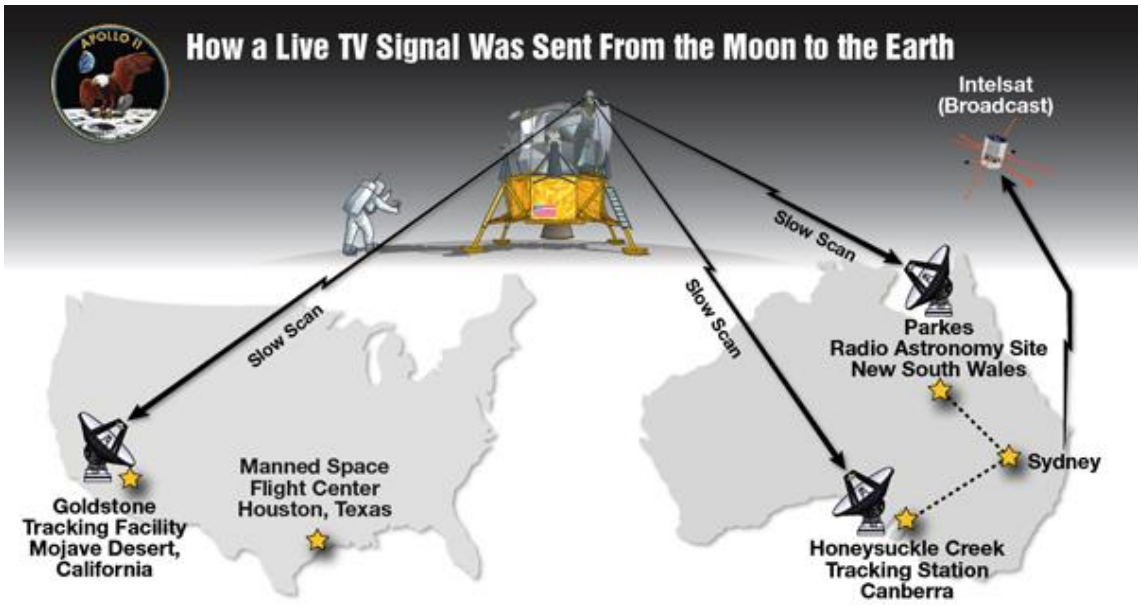
i) Datacentres

The datacentres will be held in two physical locations one being on earth and the other being on moon.

(1) Earth Datacentre

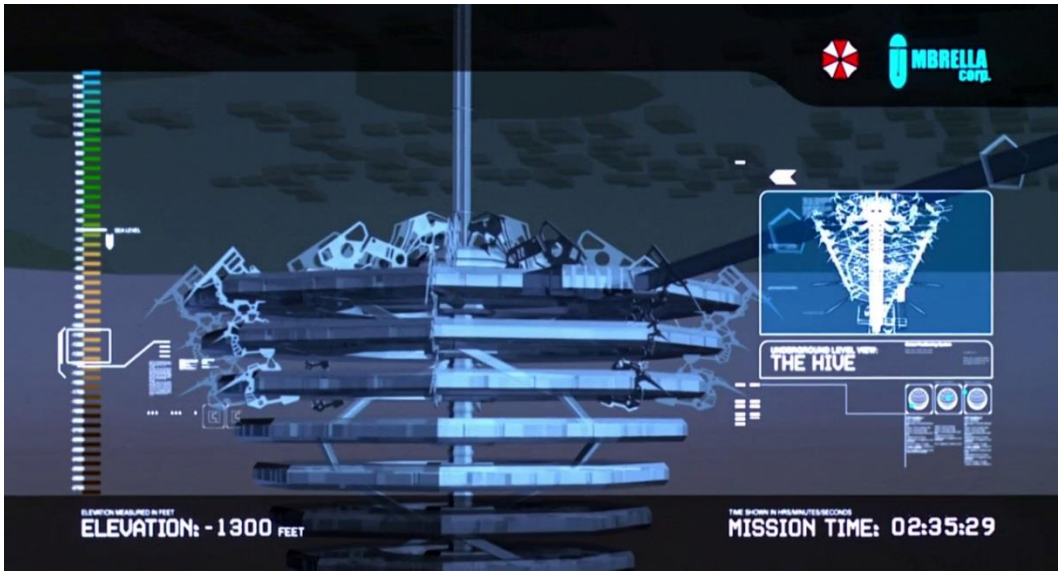
Our primary datacentre will be located underground in the Mojave Desert (Wikipedia, n.d.) this decision was made for multiple reasons.

1. As the moon landing video was broadcast back to here in 1969 it seems to be the best place for a primary uplink and as it's also close to the coast so we can utilise the underground transatlantic fibres to connect to the other satellite uplinks to provide around the clock uplink coverage and transport. I came to this conclusion by using the following pages at (StackExchange, n.d.) and this followed up to (NASA, 2009)



2. The harsh outdoor environment would make it difficult for the zombies to survive reaching the datacentre
3. We would be able to land space craft on a cleared area of the saltpans near by
4. The benefit of the labs and datacentre being underground is they will remain at a constant temperate due to the way the earth behaves as read from (Gray, 2016) and I have been personally been to world war bunkers and experienced this. They usually hover around 28 degrees
5. We can set up a vast array of solar panels above us with more than enough support of all the systems

I took most of the inspiration for the underground lab and DC from the (Resident Evil, n.d.) film series as the in theory it kept the zombies from getting out so hopefully we can stop them from getting in.



I just hope we don't end up creating an AI like the red queen in the film or we may well then all be doomed anyway

In regards to the communication to the moon as above I hope the following system has evolved from (The Optical Society, 2014) of which we can sustain 10Gbe and above links. We would also preferable have access to some (Tesla Model S, 2016) but with increased range and the (Tesla Bioweapon Defense Mode, 2016) just to protect our techs/lab staff if they need to make a getaway.

(a) Earth Datacentre- LAB

We also assume our billionaire friend is going to want to be prepared if the same unfortunate event occurs again or if he is just wanting to play it safe by having onsite labs near the DC as this is also a safe place underground. Again my inspiration has come from the Resident Evil film series as these rooms would be cooled and hermetically sealed so if an infection did occur our staff in there should be safe and be able to provide our DR plan. We also assume that we can have diverse runs from our datacentre into this room. Again we hope the AI doesn't go rouge and if you have seen the film you won't even get anything breaking in even with a very sharp axe. To also try and minimise any noise we will host any equipment in an APC NetShelter CX and as the room is cooled due to being a lab this will be fine as its also classed as a clean room of which the air quality will be high and dust free.

(2) Moon Datacentre

Our secondary datacentre will be located at the Apollo Moon landing site so we can again utilise the same uplink points that were used during the lunar landing. We assume we can replicate what we have done one earth on the moon with it all being an underground replica.

ii) Server Hardware

(1) Production Server Hardware

The server hardware I have chosen to use it Hewlett Packard due to the user friendly iLO interface for remote management and Symantec Deployment Solution (Previously HP Altiris) as a fall back if we need to PXE boot and recover or build new server hardware automatically with someone needing to be in the datacenter. In each datacentre we would deploy the following model HPE ProLiant DL580 Gen9 Server having a total of 4 in each location. We can populate these with 4 processors and up to 24 cores and a total of 6TB of RAM. In the ideal situation we would have these fully loaded and for storage have some RAID 10 SSD for persistent log storage and some NVMe devices for the software acceleration. We have decided to not go for a hyper converged system in our design as we want to be able to modular build the systems so if new technologies are invented we can easily replace the processing units and scale out if only this is required. The servers have room for more than enough room for 10Gbe connectivity we could dream of and NVidia GRID cards if we need 3D graphics via the DC in the future.

(2) Management Server Hardware

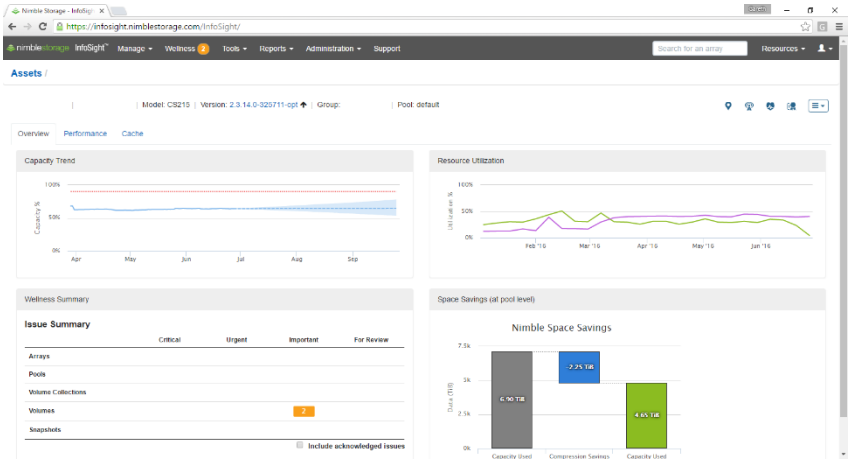
The management server hardware will be 3 i7 Intel NUCs. Due to the fact we can 'modify' the hardware we will have had Intel commission these with dual power supply inputs and 10GBe Ethernet. We also can only assume that we can now acquire 1TB NVMe tier flash and then a 5TB version for the capacity tier. The main reason for this is we need them to be portable for part of our DR plan and also to minimise space as we will be locating these in our lab. Due to this resiliency we have built in they are near production grade and the likelihood of all 3 going down at once is low. We will be hosting these in our lab.

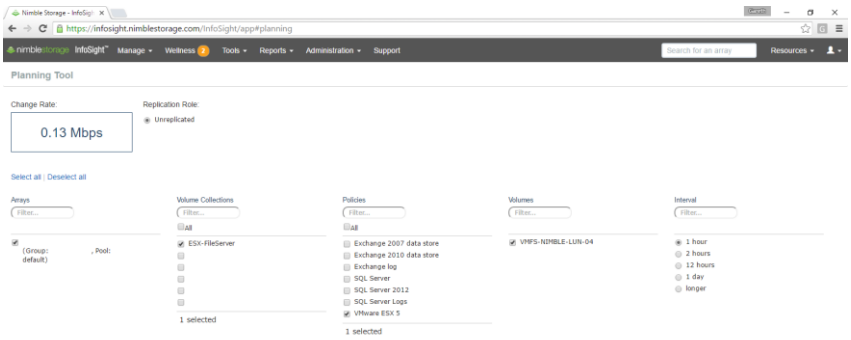
iii) Storage

We will be in fact using several types of storage hardware so we are not tied into any specific vendor so it also allows us to have mass storage and the ability to start creating tiers for a cloud based infrastructure of which our billionaire friend could then sell portions off. The other reason for multiple storage options is if one system is to fail due to a software release, hardware or maybe even if the zombies started to hack us or have morphed into viruses and attack one of the systems we could isolate this and fail over to another system in our portfolio without any major noticeable loss in performance.

(1) 1st Primary Production Storage Hardware

The first of the primary storage solutions would be Nimble Hybrid arrays as these have the ability to have an all flash shelf which we would populate in case it is ever required and in white papers been seen to perform as well as their all flash systems depending on the work load. I also feel that the Infosight analysis that will be provided back to our engineers in regards to capacity trends can allow us to plan for future growth along with the replication section to allow us to advise on our RPOs and RTOs to the board and plan the amount of bandwidth needed on our direct link to the moon. We can also utilise the VVols integration to ease replication and storage policies in manual or automated workflows. We can also cluster other units across racks if required to in the future with a single pane of glass management.





(2) 2nd Primary Production Storage Hardware

The secondary storage would be a Tintri device as we can apply most of the same above criteria but it provides us with another vendor if the Nimble device becomes unusable. The other nice thing is we can set QOS policies easily on a object basis if we sell parts off for a cloud infrastructure.

(3) 3rd Production Storage Hardware

As we are just playing it completely safe we have also decided to install a few NexSAN arrays so we can have a load of mass slow but high density storage that is enterprise grade. The other main selection for this is the (Nexsan AutoMAID, n.d.) feature that these units have where we can achieve power saving of up to 60-70% if the disks aren't in active use. This of course will aid in cooling if this ever becomes a constraint.

iv) Security

For security we will try and take as many precautions as possible

(1) Physical Security

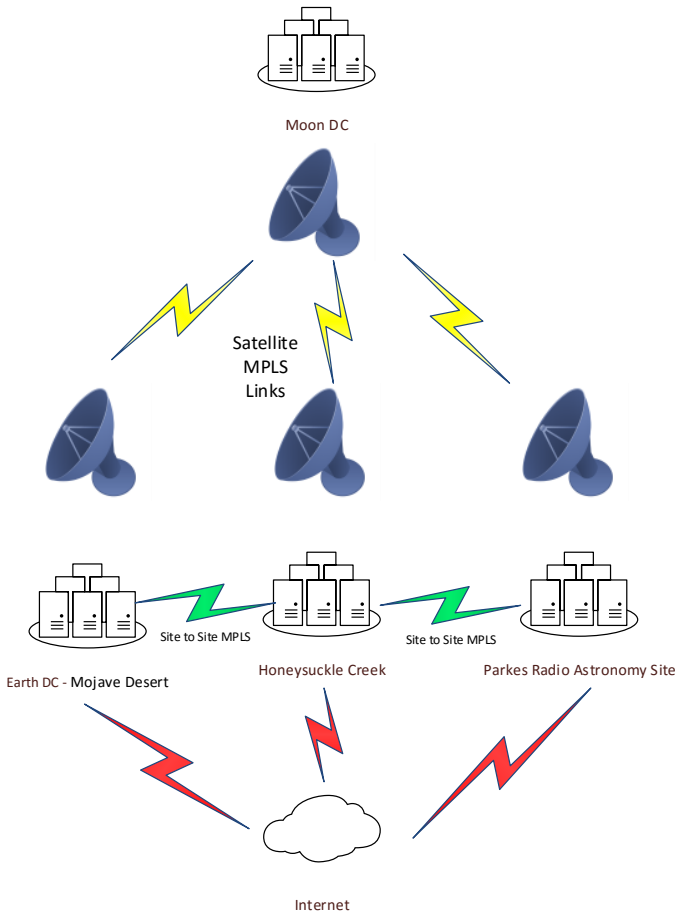
As we are already underground we are fairly secure but our uplinks should be protected by at least 3 physical barriers with gaps of which we could be flooded if required to stop an on mass of zombies or civil break down. We would also have two separate diverse escape tunnels under the ground of which we could make a get away with in our modified Tesla vehicles.

(2) Logical Security

As our staff will always have access to a up to date CMDB with valid information we will name our datacentres and VMs somewhat obscurely. This is so if the zombies or an outside force did want to hack us we are enhancing security through obscurity such as not using location names or hosted application e.g Moj-DC01. We may select a theme instead such as the location being an acronym for the data centre and the application being an identifier of that series for example we could select James Bond as a theme and their villains as the identifier so Casino Royal (CR) for the location and Oddjob as the identifier of the application making the name CR-Oddjob. As the staff can search the CMDB this will show all the links and dependencies and as they should be the best of breed engineers we are hoping this association style should be memorable.

v) Networking

Again as we have done so with the storage we have selected two vendors as we have no power, cooling or space constraints. Below is a high level connectivity diagram.



(1) 1st Production Networking Hardware

Our primary core switches will be Cisco Meraki MS420-48 having two at each site. I have chosen these switches due to their easy management and reasonable cost. It also allows for template designs as the infrastructure grows if we decided to build a larger DC or even new sites across the globe. If there is also an issue if the switch as long as it can get to the internet it can be configured and diagnosed remotely without an engineer onsite. The switches can also be managed by an API but this will need to be developed for use with our orchestration toolset. We can also utilise the virtual stacking so configuration can be make the same across sites to keep it inline.

(2) 2nd Production Networking Hardware

For old hat reliability we have chosen to use some Cisco Nexus switches as these can be managed and integration with VMware NSX and orchestration natively or via a plugin

v) Firewall and routing

For ease this time we have opted for just one vendor but two devices and having lots of them just to be safe.

(1) Datacentre and Satellite Uplink Areas

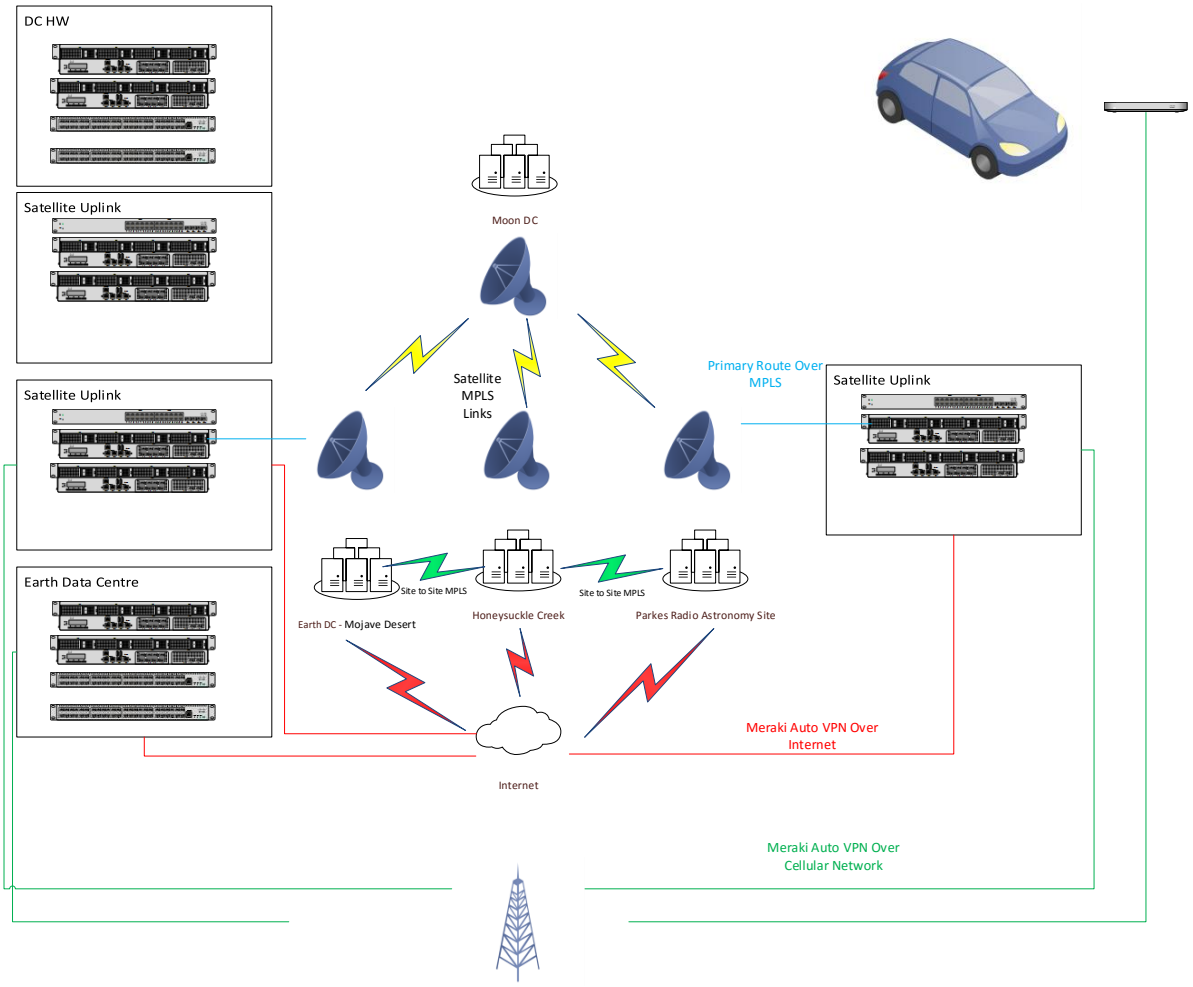
In the main areas we will be using pairs of Cisco Meraki MX600. Again our main choice for this is they can be managed over the web if required and to aid loss of any service we will be utilising the (AutoVPN, n.d.) service over the internet and 4G backup aiming for the best up time possible.

(2) Remote DC

If our staff are making a run away in the Tesla and need to get our management cluster online to seed any data, we will use Cisco Meraki MX65W's as we can utilise the Auto VPN service to connect back to one of our uplinks

(3) Routing and Auto VPN Design

Below shows a proposed design for the MPLS and Auto VPN routing



vi) Software Enhancements

In order to try and keep our storage agnostic and also keep an eye on how our data sets are performing we will be utilising PernixData FVP and also their Architect product. The main use for FVP is so we can host the databases within RAM of the host in use to eliminate the storage and network bottlenecks meaning it can run in the fastest way possible.

b) Logical Design

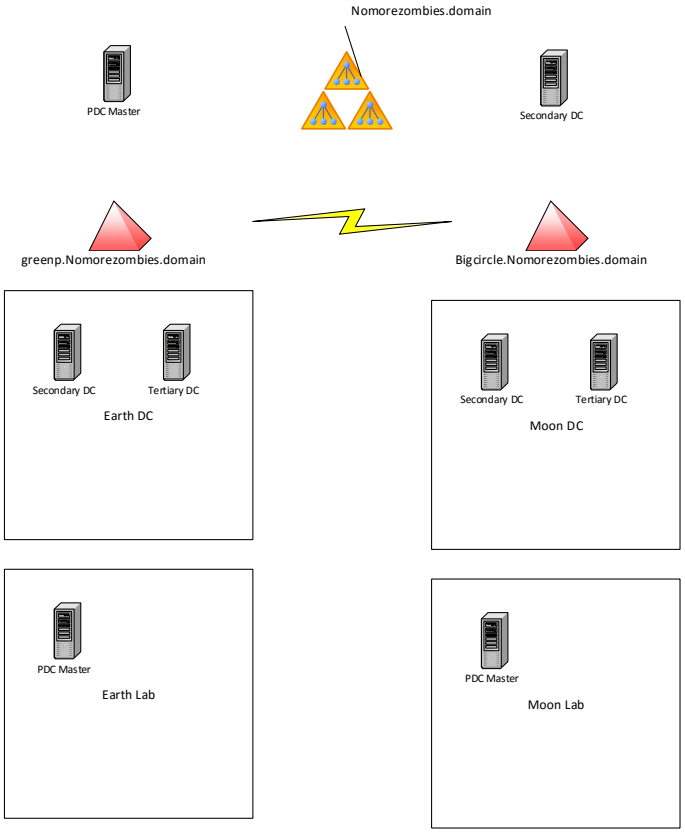
Below we have noted our logical designs to allow an easy representation of the solution

i) Logical Datacentre Design

The datacentres will be held in two physical locations one being on earth and the other being on moon.

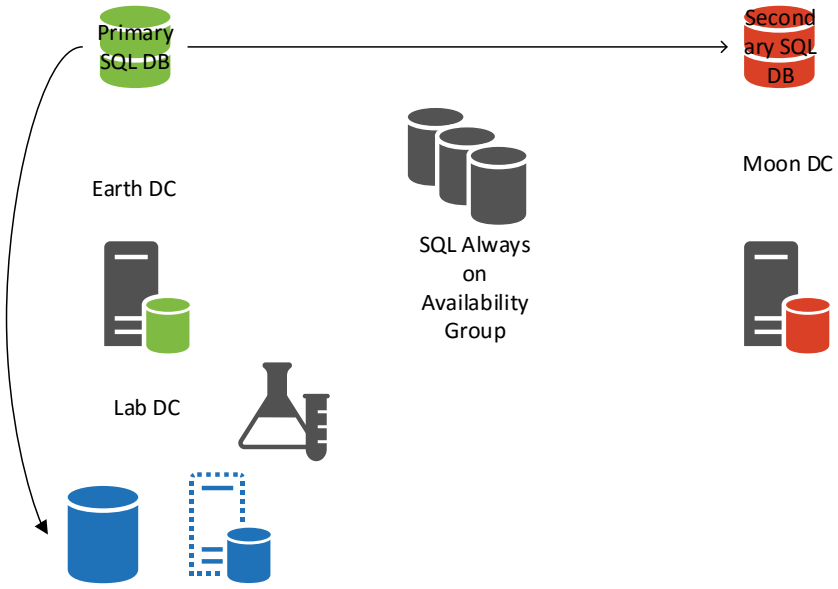
ii) AD Design

The Active Directory domain at present will be one forest and several sub domains to logically separate the areas



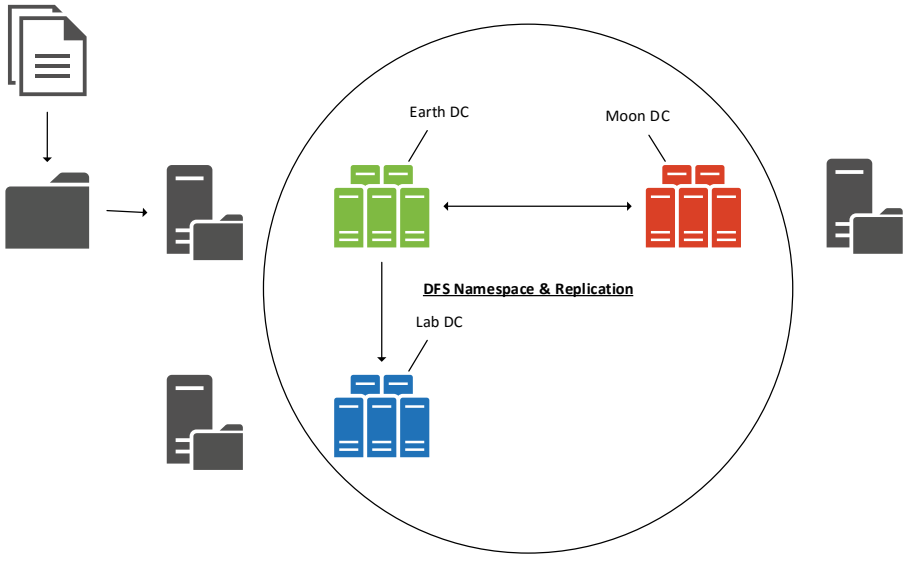
iii) Databases

The database of choice will be Microsoft SQL as we have not been provided any CPU, Disk or Memory constraints, we can also utilise the Always On Availability groups in multiple locations to ensure we always have up to date datasets. This will be used for all portions of VMware, Application, Citrix and Pernix Data management. If required, we may logically separate the databases into instances should the need arise.



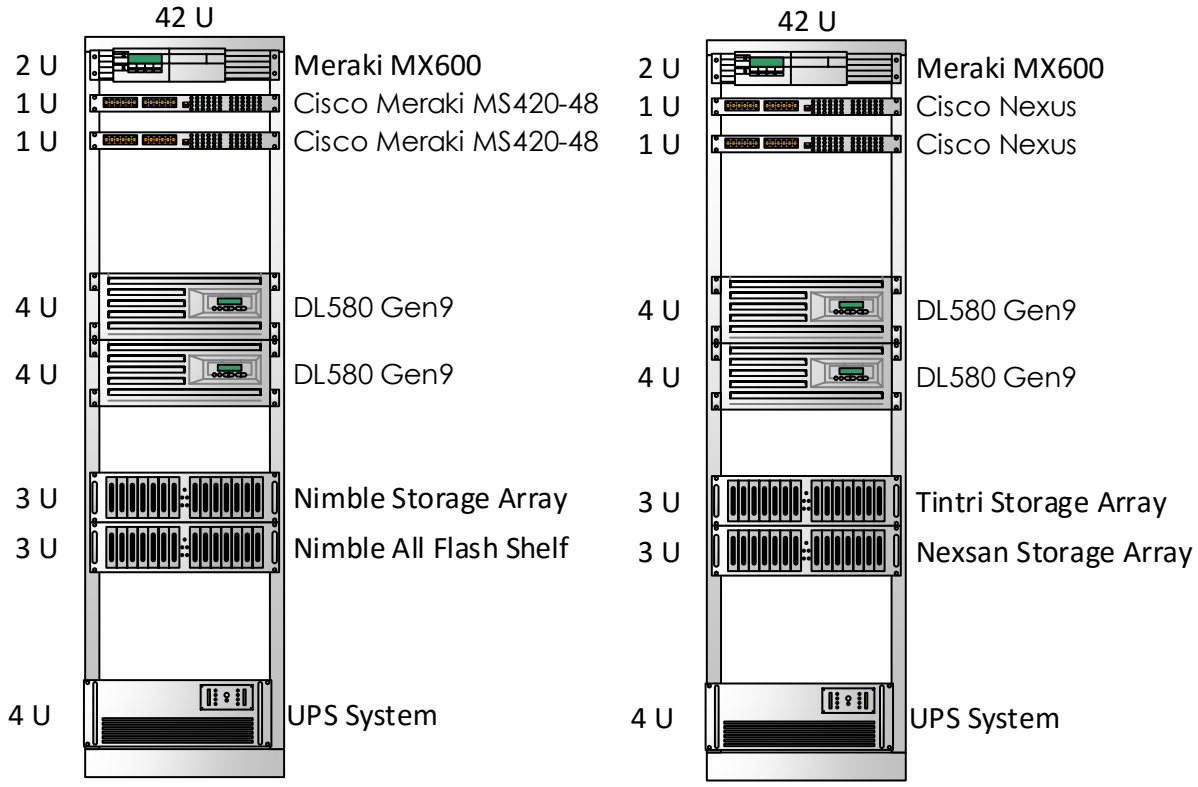
iv) File Services

The file system of choice is going to be a Windows File Server but replicated with DFS so we can attempt to have continual replication between sites if one was to fail. This is possible after checking on (DFS Replication, 2006) FAQS permitting they are in the same forest.



v) Rack Design

Below is a suggestion for our first two racks in each data centre to also allow for expansion. They are also laid out this way in case we need to isolate one.



vi) Network Design

As our data centres are not in traditional locations we have tried our best to design resiliency in where ever possible

(1) DNS

DNS is going to paramount to our system and we will be using very little static IPs. We will still be using Windows DNS services but this is so if a system is failed over to another site we do not need to re-IP to device and we can recover quickly. It also means we don't need to build in automation or constraints for servers or devices. We will only limit static IPs to specific use cases such as domain controllers, DNS, firewalls and/or gateways. As none of the systems state a current uptime or recovery period we can assume a time to live of 1 hour is acceptable but can be forced in an emergency.

(2) DHCP

We will be using DHCP on all our clients and servers which are not part of the static scope. This is to allow easy migration of servers or services between sites and endpoints of which we can quickly re-establish their connections. This has worked fine for major corporations prior to the disaster and they have managed to eradicate nearly all static IPs. Due to NDA I cannot comment on who this is.

(3) Firewall Rules

The Meraki firewalls can apply any NAT or firewall rules on a MAC and client basis due to the layer 7 monitoring. If new rules are required in an emergency, it should be fairly quick to amend any rules for the servers by selecting them in the GUI

vii) Virtual Datacentre

Although both the datacentres are in two separate locations we will be using a single vCenter and logically splitting the datacentres and then clusters due to the fact they will need access to shared resources and configuration

(1) vSphere Cluster

Each of the sites will have their own cluster of 4 nodes for the productions system so we can HA between vendor based racks. The management clusters will be 3 of the NUC nodes at each site.

(2) Storage Design

All the storage will be presented to the infrastructure in its native format for that device. The VMs will then be replicated to each site via the Nimble and then locally using Veeam to the Tintri and a backup copy to the Nexsan

(3) vCenter Server Design

The vCenter server will be a singular Windows VM. I have decided to not use an appliance as I will want to run update manager on here to and I can leverage the SQL always on availability if I need to run the replicated server on another node in the cluster or the other site.

(4) vCloud Suite

We are going to include the vCloud enterprise suite so we have the ability to fully monitor, maintain and manage the infrastructure. This will allow us to use vRealize Automation for orchestration along with vRealize operations to monitor our infrastructures performance. Log insight manager will allow us to track any changes and aid in log compliance for security.

(5) Multi Tenancy

As we have used the vCloud enterprise tool set it means we can set up a framework to allow the system to be used for multi tenancy if the need arises in the future

(6) Orchestration

We will utilise vRealize Automation as suggested before so we can create consistent VMs and configure the majority of the work flow. Some of this may end up using Docker to create the web servers upon the Photon OS

(7) Patches and Updates

We will deploy a Windows WSUS server to manage patches on our Windows servers of which when a service is commissioned if they are highly available we will have them auto update on separate weeks during non-core hours. We will have the VMware update manager running on our vCenter server

(8) Accessing the work load

Day to day as the application appears to be accessed by the web servers we will send all the clients to the earth DC as bandwidth around earth and the DC should be sufficient. If we end up in a failover state to the Moon we will have the users access the system via Citrix so this reduces the data traversing down the link back to earth. We will also include any productivity suites within the Citrix farm so any documents can also be modified as if they were local to the user and application.

c) Work Load

All we know about our most critical application HumanityLink is that it consists of three front end web servers, one database, and two application servers. Performance of this software is paramount so we have designed the infrastructure to support all of its assumed requirements. We have assumed as before the end user will digest the software via a web browser. As we have over compensated on any if not all of the components the system should be able to be scaled in any direction.

d) Backup Design

For the purpose of being agnostic where possible we have decided to utilise the replication and snapshots built into our Primary storage device being the Nimble on top of this we will be replicating the VMs with Veeam to the Tintri and a copy job to the Nexsan. We decided against VMware's SRM as the SRA adaptor usually creates a vendor or software level tie in and may cause delays in the future.

e) Update Design

We have already eluded to this before but we will be utilising WSUS and VMware's update manager for our major updates. The VMware update manage can also perform the HP host updates if required. The hardware updates will be manually applied to our non-primary datacentre first to avoid any outages.

c) Monitoring Design

For monitoring we will be monitoring the virtual elements from VMware's Operations manager. For anything else we will be utilising PRTG as it has the ability to be scripted for any plugins we do not have available. Any alerts from this system will be emailed and after 5 minutes if not responded to we will then send these by SMS. When possible we will also look at a POC of VMTurbo to see if this can add value for our engineering staff.

3) Disaster Recovery Summary

a) Disaster Recovery Overview

We have decided to go a little overboard on the DR design whilst we only have one datacentre on earth and then rely on the moon. Below we have outlined a few high level plans we can use to initiate DR.

i) Physical or Software Failure in primary DC

This is the most logical event to take our datacentres offline, when this occurs we will use the elements within Veeam to perform a (Planned Failover, 2016), once this is complete most the VMs should be accessible quickly as we are hoping when the system collects a DHCP address DNS should then register its new IP.

ii) OH NO! Another outbreak or attack

If for any reason the zombies reappear and try to attack us or our datacentre we will invoke the bug out operation. This will involve the staff in the lab (assumed its run 24/7/365) to press the big red button which will initiate a shutdown of the 3 NUC management cluster of which we will aim for this to be down with 2 minutes. This will allow any saved work to hopefully sync to the SQL and DFS instances on there. Once shut down the staff should place them in the prepared flight case and head straight to the escape ramps housing the already charged Teslas. These will have already been fitted with special 240v invertors to run our equipment. As the Tesla has an internet/WiFi subscription we will utilise this to link back to the moon/satellite sub bases. The 'bug out bag' will contain the following equipment to facilitate this:-

- 6 additional NUC PSUs so staff don't need to disconnect the current ones
- All the required network uplinks and media convertors
- 1 Meraki Cisco MX65W
- 1 Wireless Bridge configured to link to the cars WiFi

Hopefully there is more than one member of staff escaping so whilst one is driving the other can put together all the equipment. Once this has established the AutoVPN the moon base IT staff can then ensure everything is syncing whilst the earth staff drive to the designated safe house.

4) Final Thoughts

a) What would I have done different

If I had more time I would have investigated more networking elements and planned out the VLANs. Due to time constraints I have to exclude some elements and provide a more high level design in areas. In the next challenge I will ask the judges more questions as I have made way too many assumptions such as processing power needed, having access to the internet and even an email system! I would also prefer to plan out VM placement so I can show the naming conventions and plan for backups/recovery better with justification. I feel I am also missing much of the automation element and its work flows or even demonstrating these at a high level. I also need to learn Docker or Photon OS more.

References

AutoVPN. (n.d.). *MPLS Failover to Meraki Auto VPN*. Retrieved from MPLS Failover to Meraki Auto VPN: https://documentation.meraki.com/MX-Z/Deployment_Guides/MPLS_Failover_to_Meraki_Auto_VPN

DFS Replication. (2006, October 16). *DFS Replication: Frequently Asked Questions (FAQ)*. Retrieved from DFS Replication: Frequently Asked Questions (FAQ): https://technet.microsoft.com/en-us/library/cc773238(v=ws.10).aspx#BKMK_000

Gray, J. (2016, April 12). *Underground Construction*. Retrieved from Sustainablebuild.co.uk: http://www.sustainablebuild.co.uk/constructionunderground.html

NASA. (2009, 07 16). *Apollo 11 Tape Restoration Project: Briefing Materials*. Retrieved from NASA: http://www.nasa.gov/mission_pages/apollo/40th/apollo11_conference.html

Nexsan AutoMAID. (n.d.). *Nexsan AutoMAID™*. Retrieved from Nasi: http://www.nasi.com/nexsan-automaid.php

Pexels. (n.d.). *Pexels.com Image Gallery*. Retrieved from Pexels: https://www.pexels.com/photo/earth-space-cosmos-5439/

Planned Failover. (2016, 5 4). Retrieved from Planned Failover: https://helpcenter.veeam.com/backup/vsphere/planned_failover.html

Resident Evil. (n.d.). *Resident Evil (film series)*. Retrieved from Wikepedia: https://en.wikipedia.org/wiki/Resident_Evil_(film_series)

StackExchange. (n.d.). *How did NASA achieve their live TV broadcast in 1969?* Retrieved from StackExchange: http://space.stackexchange.com/questions/2993/how-did-nasa-achieve-their-live-tv-broadcast-in-1969

Tesla Bioweapon Defense Mode. (2016, May 2). *Putting the Tesla HEPA Filter and Bioweapon Defense Mode to the Test*. Retrieved from Tesla Motors: https://www.teslamotors.com/en_GB/blog/putting-tesla-hepa-filter-and-bioweapon-defense-mode-to-the-test

Tesla Model S. (2016). *Model S*. Retrieved from Tesla: https://www.teslamotors.com/en_GB/models

The Optical Society. (2014, May 22). *First broadband wireless connection ... to the moon: Record-shattering Earth-to-Moon uplink*. Retrieved from sciencedaily.com: https://www.sciencedaily.com/releases/2014/05/140522104949.htm & http://www.theregister.co.uk/2011/09/26/space_optic/

Wikipedia. (n.d.). *Mojave Desert*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Mojave_Desert

Disclaimer

The view expressed in this document are my own and do not necessarily reflect the views of my current, previous or future employer(s). This is a fictional design and some elements may not work correctly within your infrastructure. All data and information provided on this this document is for informational purposes only. I make no representations as to accuracy, completeness, currentness, suitability, or validity of any information throughout the document & will not be liable for any errors, omissions, or delays in this information or any losses, injuries, or damages arising from its display or use. All information is provided on an as-is basis.

Revision History

Version	Performed By	Date / Time	Comment	Action
0.1	Gareth Edwards	26/07/2016	Template Created	Initial Action
0.2	Gareth Edwards	26/07/2016	Initial body created	Design forming
0.3	Gareth Edwards	27/07/2016	More design formed and diagrams formed	Further work to design
1.0	Gareth Edwards	28/07/2016	Final Panic for release	Included more screenshots and quick proof read
1.1	Gareth Edwards	28/07/2016	Extra Panic	Added security section back in as human error deleted it!

End of document