HumanityLink 2.0 aka HLDeuce

vDM Challenge1: A 3-Site Design

Nigel Hickey; VCIX6-DTM

@vCenterNerd

TABLE OF CONTENTS

1 DOCUMENT CONTROL

Preparation

Action	Name	Date
Technical Content	Nigel Hickey	7/1/2017
Formatting	Nigel Hickey	7/4/2017

Release

Version	Date Released	Change Notice	Pages Affected	Remarks
1.0	7/1/2017	Internal	All	Initial Draft
1.1	7/4/2017	VDM Release	All	VDM Release

Distribution

Name	Organization	Role	E-mail
Eric Wright	vDM	Head Canadian, Eh!	eric@discoposse.com
Angelo Luciani	vDM	Chief Ginger Officer	Aluciani@gmail.com
Melissa Palmer	vDM	Dr. Evil's Sister	vmiss33@gmail.com
Byron Schaller	vDM	Judge	byron.schaller@gmail.com
Rebecca Fitzhugh	vDM	Judge	rmfitzhugh@gmail.com
Lior Kamrat	vDM	Judge	https://twitter.com/LiorKamrat
Nigel Hickey	vCenterNerd Consulting	Architect / Engineer	Nigel.Hickey@gmail..com

2 PROJECT OVERVIEW

2.1 INTRODUCTION & SCOPE

The humans on Earth have been very busy recolonizing the planet as well as working on an army of robots to help carry out global terraforming efforts. Because of this, Mr. Billionaire has engaged vCenterNerd Consulting to design and document a 3-site architecture that will support the newest version of HumanityLink 2.0 aka HLDeuce. HLDeuce will be deployed with the potential to support unknown workloads, easily scalable & repeatable, and built with resilience in as many layers as possible. HLDeuce will also include new features to support robot maintenance, scheduling, and operations.

vCenterNerd Consulting will look to design a 3-site architecture that is highly available, secure, and scalable by utilizing 2 Physical datacenters, and 1 Cloud datacenter at Amazon Web Services (AWS). HLDeuce will be installed leveraging EC2 Container Service and will run 60% of its workload in the AWS Datacenter and utilize Auto Scaling as well as Global Availability Zones to be scalable & accessible from literally anywhere on Earth. The other 40% of the HLDeuce workloads will run in the other 2 Datacenters (20% each) along with any other required workloads.

Both Physical datacenters will use the same hardware as well as configurations to ease the impact of disaster by allowing full recovery at either Datacenter.

2.2 DESIGN QUALITIES

Design decisions, accompanied by justification for and impact of each decision, are included throughout the design. Design choices are compared with their impact against certain characteristics and summarized below.

Availability

Indicates the effect of a choice on the ability of a technology and the related infrastructure to achieve highly available operation and to sustain operation during system failures. HLDeuce must be highly available and avoid single points of failure.

Performance

Reflects whether the option has a positive or negative impact on the overall infrastructure performance. HLDeuce must run at the highest performance possible to support Humans and Robots as terraforming efforts continue.

Manageability

Relates the effect of a choice on overall infrastructure manageability. IT staff are in short supply as well as many are refocused on terraforming efforts, so ease of management and configuration should be easily understood and teachable.

Security

Reflects whether the option has a positive or negative impact on overall infrastructure security. With most zombies gone now the focus is now on hackers or those that wish to see HLDeuce & humanitarian efforts fail.

Recoverability

Indicates the effect of a choice on the ability to recover from a catastrophic event. Since humans and now robots will rely on HLDeuce even more, we will need to be able to recover from disastrous situations.

2.3 REQUIREMENTS, CONSTRAINTS, ASSUMPTIONS, AND RISKS

2.3.1 Requirements

Number	Description	Design Quality
R01	Build a 3-site Architecture	Manageability, Availability
R02	Provide resiliency to Architecture	Availability, Recoverability
R03	Ensure HLDeuce is highly available	Availability
R04	Ensure high performance of HLDeuce	Availability, Performance
R05	Ensure systems & datacenter security	Security, Recoverability

2.3.2 Constraints

Number	Description	Design Quality
C01	Datacenter Locations are on Earth	Manageability, Availability
C02	No limitations on Hypervisor, hardware, network stack, or applications	Manageability, Availability, Performance, Security, Recoverability
C03	Human efforts mainly focused on recolonization	Manageability
C04	HLDeuce runs as a MEAN stack application	Manageability, Availability, Performance

2.3.3 Assumptions

Number	Description	Design Quality
A01	Humans are too busy to configure all systems by hand	Manageability
A02	Vendor hardware is available	Availability, Performance
A03	Earth-like environmental conditions exist (power/cooling/etc)	Availability, Performance, Recoverability
A04	Abandoned datacenters on Earth are not available	Availability, Recoverability
A05	Software & Licensing for all products used is available	Manageability, Availability
A06	WAN connections between datacenters are at least 100mbps & redundant	Manageability, Availability, Performance, Recoverability
A07	AWS still has operating datacenters in global availability zones	Manageability, Availability, Performance, Recoverability

2.3.4 Risks

Number	Description	Design Quality
R01	Future workloads and/or datacenter expansion is unknown	Manageability, Security
R02	Hardware failures can occur at datacenters	Availability, Recoverability
R03	OS and/or Application failures can occur at datacenters	Availability, Recoverability
R04	Zombies could be near datacenters	Security, Recoverability
R05	Human efforts mainly focused on recolonization	Manageability

2.4 DATACENTER LOCATIONS

Location	City	Country	DC Name
MoD Machrihanish	Machrihanish	Scotland	MAC
Devonport Naval Base	Auckland	New Zealand	DNB
Amazon Web Services	AWS Global Availability Zones	USA	AWS

2.4.1 MoD Machrihanish (MAC)

The location of the first datacenter will be just outside of Machrihanish, Scotland at MoD Machrihanish (formally known as RAF Machrihanish). Machrihanish is the site of a former Royal Air Force station located 3 nautical miles west of Campbeltown, Scotland. Being that this was a secluded location military base supporting US Navy Seals, RAF units, and the US Naval Special Warfare Command (NSWC) until 2012, it can be assumed that this facility can support IT Infrastructure and/or revert to its intended military use if needed. The location is also ocean facing allowing for access to fresh water, farming, and raw materials. Environmental threats like hurricanes and earthquakes are low in this region. Most Zombies, like humans, do not like the sounds of bagpipes nor haggis so this should further deter them from this area. [R01]

2.4.2 Devonport Naval Base (DNB)

Our second datacenter will be located in Auckland, NZ utilizing the infrastructure at Devonport Naval Base. This base carries some similar characteristics as MoD Machrihanish. The base also has a modern power converter system to supply substantial power to berthed Navy ships. This power setup was only deployed in the late 2000s so we can assume power requirements for our datacenter can be met, for now and in the future. Being an island, New Zealand can also offer the same fresh water, farming and access to natural resources as MoD Machrihanish.

Both the MAC & DNB datacenters will be able to run HLDeuce workloads, as well as other needed applications to support Robot manufacturing, upgrades, etc, and will act as failover locations when workloads in AWS are unavailable. The AWS DC will be the primary location for running HumanityLink 2.0 aka HLDeuce. [R01]

2.4.3 Amazon Web Services (AWS)

Our third and last datacenter will be hosted in Amazon Web Services or AWS. AWS will be the primary location for our HumanityLink Software. AWS will allow us to run the new version of HumanityLink, HLDeuce, on their public cloud platform as well as keep the application highly available across global regions, run on high performance systems, be scalable, and allow support for managing the AWS infrastructure as code by leveraging Terraform.

HLDeuce will run in an AWS Virtual Private Cloud (VPC) across 2 Availability Zones. AWS Auto Scaling will be leveraged where Web, Database, and Application servers that support HLDeuce can be placed in Auto Scaling Groups (ASG). These ASGs will work in conjunction with AWS Lambda & CloudWatch; for code execution based from alerts/rules; AWS S3 buckets for storing Lambda functions and configurations as well as utilizing AWS CloudFormation Templates to deploy initial infrastructure. Internal & External Load Balancers (ILB & ELB) will be used between AWS Availability Zones.

Palo Alto VM-Series Firewall for AWS will also be used to help protect our AWS workloads. The VM-Series Firewall for AWS will also leverage ASGs to be able to scale with our HLDeuce application. This firewall was chosen due to its ease of deployment with bootstrap configuration files that can be placed in S3 buckets to create a repeatable and streamlined process of deploying new VM-Series firewalls. This deployment can also help protect our mobile workforce in the future (Robots) by using Palo Alto's GlobalProtect that works in conjunction with the VM-series Firewall for AWS. [R01] [R03] [R04]

3 INFRASTRUCTURE DESIGN

3.1 HOST DESIGN

The implementation of Dell R730XD servers will be used at both the MAC & DNB datacenters. These systems will be configured with VMware vSphere 6.5 and leverage VSAN clusters. 3 Hosts will provide the Management cluster & 6 Hosts will provide the Compute cluster. [R02] [R04]

Processor	2 x Intel Xeon E5-2630 v4 2.2GHz 10 Core CPU
Memory	8 x 32GB RDIMM 2133, Total of 256GB per Host
Hard Drive(s)	2 x 800GB SAS SSD Write Intensive (Cache Tier) 14 x 1.6TB SATA SSD Read Intensive (Capacity Tier)
Network Card(s)	2 x Intel x520 Dual Port 10GB SFP+ Network Adapter w/Optics 1 x Intel i350 Quad Port 1GB Network Daughter Card, LoM
SATA DOM	1 x 64GB SATA DOM (OS Install)
LoM	iDRAC 8 Enterprise Remote Access Controller

3.2 CLUSTER DESIGN

3.2.1 vSphere

VMware vSphere 6.5d Build 5310538 will be deployed in the MAC & DNB datacenters. Each datacenter will have a single VMware Datacenter object containing two separate VMware Clusters, 1 Management Cluster with 3 ESXi nodes & 1 Compute Cluster with 6 ESXi nodes. The Mgmt. cluster will support AD, SQL, VCSA, and NSX while the Compute cluster will support all other server workloads that pertain to HLDeuce (db, web, and app servers). The following vSphere cluster level features will be utilized:

- VMware vMotion
- VMware High Availability (HA)
- VMware vSphere Distributed Resource Scheduler (DRS)
- VMware VSAN

3.2.2 vCenter

One vCenter Server Appliance (VCSA) and one external Platform Services Controller (PSC) will be deployed in the MAC & DNB datacenters. Keeping the PSC external will allow other services to remain running if the VCSA was to go offline or crash. This design will also allow for VCSA expansion (adding more VCSAs) as well as being able to leverage Enhanced Linked Mode, when needed. The default SSO domain will be used: vsphere.local. VMware Update Manager (VUM) will be used and is now embedded in the 6.5 version of the VCSA. [R02]

VM	Description	vCPU	RAM	Disk
MAC-VCSA01	VCSA (Small)	4	16GB	290GB
MAC-PSC01	PSC	2	4GB	60GB

VM	Description	vCPU	RAM	Disk
DNB-VCSA01	VCSA (Small)	4	16GB	290GB
DNB-PSC01	PSC	2	4GB	60GB

3.2.3 SRM & vSphere Replication

To ensure we have failure protection of the HLDeuce application when running in the MAC & DNB datacenters, we will use Site Recovery Manager (SRM) and vSphere Replication to replicate the HLDeuce VMs between sites. HLDeuce will be replicated from MAC (Protected site) to DNB (Recovery Site) and if any other VMs are discovered to be mission critical, we can add those to SRM also. SRM will use the embedded version of vProgress versus an external SQL for ease of management and deployment. [R05]

VM	Description	vCPU	RAM	Disk
MAC-SRM01	SRM at Protected Site	4	16GB	290GB
MAC-VSR01	vSphere Replication Appliance	2	4GB	20GB
DNB-SRM01	SRM at Protected Site	4	16GB	290GB
DNB-VSR01	vSphere Replication Appliance	2	4GB	20GB

3.3 STORAGE DESIGN

VMware Virtual SAN (VSAN) was selected based on the need for a Hyper-converged storage model that could withstand failures as well as supporting a scale out, or up & down growth plan. VSAN is tightly coupled with the underlying VMware ESXi hypervisor and provides an ease of implementation and management to the humans supporting these systems.

The VSAN cluster configuration will use 2 disk groups on each server, taking up 16 disk slots on each. This will leave 8 slots open for future expansion*. [R02]

Disk Group	Disk Counts
Group 1	1 x 800GB SSD & 7 x 1.2TB SSD
Group 2	1 x 800GB SSD & 7 x 1.2TB SSD
Group 3*	Future Expansion*

3.4 NETWORK DESIGN

Two Cisco Nexus 92160YC-X Series ToR switches will be setup for 10GB at both the MAC & DNB datacenters to support the VMware vSphere clusters. Having 2 switches in each datacenter will increase redundancy.

The Cisco ASA 5585-X with FirePOWER SSP-60 next-gen firewall will be used in both the MAC & DNB datacenters to provide network security from malicious threats and the VPN connection between the MAC, DNB, and AWS datacenters.

3.4.1 NSX

VMware NSX 6.3 Will be used to operate the logical networks. This will consist of one NSX Mgr, three NSX controllers, and one Edge Gateway at each datacenter for a total of 10 NSX devices. NSX enables the creation of entire networks in software and embeds them in the hypervisor layer, abstracted from the underlying physical hardware. This setup can allow for rapid, non-disruptive network changes. [R02] [R05]

NSX VM	Description	vCPU	RAM	Disk
MAC-NSX-MGR01	NSX Manager (MAC)	4	16GB	60GB
MAC-NSX-EDG01	NSX Edge Gateway (MAC)	2	1GB	2GB
MAC-NSX-CTRL01	NSX Controller 1	4	4GB	20GB
MAC-NSX-CTRL02	NSX Controller 2	4	4GB	20GB
MAC-NSX-CTRL03	NSX Controller 3	4	4GB	20GB
DNB-NSX-MGR01	NSX Manager (DNB)	4	16GB	60GB
DNB-NSX-EDG01	NSX Edge Gateway (DNB)	2	1GB	2GB
DNB-NSX-CTRL01	NSX Controller 4	4	4GB	20GB
DNB-NSX-CTRL02	NSX Controller 5	4	4GB	20GB
DNB-NSX-CTRL03	NSX Controller 6	4	4GB	20GB

VMware Distributed Switches will be utilized for Management, vMotion, VSAN and VM traffic types and will be deployed the same at both MAC & DNB datacenters as follows:

Port Name	Port Group #
Management	1
VSAN	2
vMotion	3
VM	4
HumanityLink (HLDeuce)	5

3.4.2 VLANs

Cluster Network traffic will be segmented into the following VLANs:

VLAN Name	VLAN ID
Management	100
VSAN	200
vMotion	300
VM	400

3.5 VIRTUAL MACHINE DESIGN

The vSphere infrastructure can provide VMs for Windows & Linux operating systems. Virtual Machine templates will be used whenever possible to speed the deployment process of new VMs in the environment. We will also be able to leverage Terraform's vSphere provider to interact with vSphere and create VMs from templates in our environment.

3.5.1 Active Directory

AD will be used and deployed on three Windows 2012 R2 virtual machines. We will begin with one AD server in each datacenter with the intention to expand AD when required or for redundancy. Each AD controller will provide DHCP as well as DNS.

VM	Description	vCPU	RAM	Disk
MAC-ADS01	AD server w/ DNS & DHCP	2	8GB	80GB
DNB-ADS01	AD server w/ DNS & DHCP	2	8GB	80GB
AWS-ADS01	AD server w/ DNS & DHCP	2	8GB	80GB

3.6 HUMANITYLINK DESIGN (HLDEUCE)

The HumanityLink 2.0 (HLDeuce) will run on 7 virtual machines within each datacenter. Having these systems in each DC will allow us to use MAC & DNB to run HLDeuce when AWS is busy, unavailable, or if access to HLDeuce locally is needed to support robot operations in each site/region. [R01] [R02] [R03] [R04]

MAC Datacenter VMs:

VM	Description	vCPU	RAM	Disk
MAC-HLD-WEB01	HLDeuce Web Server 1	8	16GB	40GB
MAC-HLD-WEB02	HLDeuce Web Server 2	8	16GB	40GB
MAC-HLD-WEB03	HLDeuce Web Server 3	8	16GB	40GB
MAC-HLD-DB01	HLDeuce DB Server 1	12	128GB	500GB
MAC-HLD-DB02	HLDeuce DB Server 2	12	128GB	500GB
MAC-HLD-APP01	HLDeuce App Server 1	22	64GB	50GB
MAC-HLD-APP02	HLDeuce App Server 2	22	64GB	50GB

DNB Datacenter VMs:

VM	Description	vCPU	RAM	Disk
DNB-HLD-WEB01	HLDeuce Web Server 1	8	16GB	40GB
DNB-HLD-WEB02	HLDeuce Web Server 2	8	16GB	40GB
DNB-HLD-WEB03	HLDeuce Web Server 3	8	16GB	40GB
DNB-HLD-DB01	HLDeuce DB Server 1	12	128GB	500GB
DNB-HLD-DB02	HLDeuce DB Server 2	12	128GB	500GB
DNB-HLD-APP01	HLDeuce App Server 1	22	64GB	50GB
DNB-HLD-APP02	HLDeuce App Server 2	22	64GB	50GB

3.7 BACKUPS

Veeam Backup & Replication version 9.5 will be used to protect the VMs within the vSphere environment. We will also leverage Veeam Cloud Connect to store backups off-site from the datacenters. Veeam will be installed on a virtual machine in both the MAC & DNB datacenters with the below specs:

VM	Description	vCPU	RAM	Disk
MAC-VEE01	Veeam Server	2	8GB	500GB
DNB-VEE01	Veeam Server	2	8GB	500GB

Incremental Backups will be run daily for HLDeuce virtual machines at 1am. Next all Active directory servers will run backups once HLDeuce jobs are complete. After those are completed, Veeam will then backup all remaining virtual machines that require backups.

Full backups will run weekly on Mondays and all retention policies will be setup for one week. [R02]

4 REFERENCES

MoD Machrihanish
https://en.wikipedia.org/wiki/RAF_Machrihanish

Devonport Naval Base
https://en.wikipedia.org/wiki/Devonport_Naval_Base

VCDX Boot Camp (book)
Arrasjid, J. Y., Lin, B., & Khalil, M. (2013)

Jason Langer
Phone calls & emails about Host Designs & VSAN

Katarina Wagnerova
Referencing her HumanityLink Servers design/scope from Season 4; Challenge 1

vSphere Documentation
https://docs.vmware.com/en/VMware-vSphere/index.html

VSAN Documentation
https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.virtualsan.doc/GUID-AEF15062-1ED9-4E2B-BA12-A5CE0932B976.html

NSX for vSphere
https://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html

Cisco Firewall
http://www.cisco.com/c/en/us/support/security/asa-5585-x-firepower-ssp-10/model.html

Cisco Switches
http://www.cisco.com/c/en/us/products/switches/nexus-92160yc-switch/index.html

Palo Alto Networks | GlobalProtect - Scalable Remote Access for AWS White Paper
https://www.paloaltonetworks.com/resources/whitepapers/building-scalable-globalprotect-deployment

Next Generation Security with VMware® NSX and Palo Alto Networks® VM-Series
https://www.paloaltonetworks.com/resources/whitepapers/vm-series-integration-technical-whitepaper

Adding a Hardware Virtual Private Gateway to Your VPC
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

Terraform Providers (AWS & vSphere)
https://www.terraform.io/docs/providers/aws/index.html
https://www.terraform.io/docs/providers/vsphere/index.html

Veeam Backup & Replication 9.5
https://helpcenter.veeam.com/docs/backup/vsphere/system_requirements.html?ver=95