Architecture Design Document
VirtualDesignMaster - Season 2

Challenge 4

Prepared by: Daemon Behr

Date: 2014–08-5

Revision History

Date	Rev	Author	Comments	Reviewers
2014-08-5	R1	Daemon Behr	Challenge 4	

Design Subject Matter Experts

The following people provided key input into this design.

Name	Email Address	Role/Comments
Daemon Behr	daemonbehr@gmail.com	Infrastructure Architect

Contents

1. Purpose and Overview

1.1 Executive Summary

We've been dealing with the aftermath of a second round of the zombie outbreak. We've designed the systems to build spaceships, which are evacuating what's left of the human race from the earth. We've built the infrastructure to support our new civilization on the moon. We've also tried to prepare what's left of the earth in case there is another round of the outbreak, by fortifying islands across the world by deploying infrastructure remotely.

We now must truly prepare for our journey to Mars. Our large ships from earth are retrofitted on the moon for the long journey. They will be part living quarters, part laboratory space, and part shipping container when they are ready to leave the moon. The journey will take anywhere from three to six months depending on when the ship is launched. Each ship will carry people and equipment to begin settlement. Ships are designed to land on Mars and become temporary housing until permanent structures are finished.

As such, we must design an infrastructure to completely support all of these environments. It must also continue to be suitable when the ships reach Mars. Each ship's systems will be connected to an environment we are calling The Elysium Grid, which will be the foundation of the new Martian infrastructure. Of course, power, space, and cooling are all limited for the journey.

You will be each be given one server, a Dell M610 with 12 GB of RAM hosted by BareMetalCloud. Each competitor must create a nested deployment of vSphere hosts (you may use any production version you'd like, no beta software). In addition, the architecture must include vCenter, vCloud Director, vCenter Orchestrator and your entire guest and management networks running on Distributed Virtual Switches. You also must have at least two active, accessible guests available in your environment, including at least one Linux and one Windows. Any version or distribution is allowed.

The second part of your challenge is to show a true Virtual Design Master understands infrastructure from end to end. You must deploy a working overlay networking infrastructure such as VXLAN in your host environment. You must also illustrate deployment of Docker inside your host environment.

You must provide documentation on your environment, including host and network topologies, IP information, and root level credentials so the judges can access the environment. Please make sure to document and justify your design decisions. Don't feel limited by the design minimums, feel free to add extra components and software as you see fit, provided you have met the requirements.

1.2 Summary Analysis

The purpose of this design is to build an extremely small-scale environment that has the potential to expand to a very large one. Flexibility and feature richness is key, however functionality also needs to be proven so some concessions will need to be made. The design must have the scaling framework in place to expand when the hardware is available.

1.3 Design Interpretation

There are many constraints to the deployment of the infrastructure. The first one being that it needs to be a fully nested infrastructure. This limits and directs the design to mirror a full infrastructure including network, storage, compute and management framework. Components for each one of these were chosen based on resource utilization overhead, functionality and role combination. Pre-built appliances

were used when available to limit deployment and configuration time. Appliances with embedded databases were preferred in order to minimize resource usage and component sprawl. When Windows is “required”, the version chosen was the least resource intensive that met the functional requirements. Several roles were integrated in a single VM (which contravenes best practice), with the understanding that when resources become available they will be separated.

Since there are many components, management and visibility to all of them from a single pane of glass is not inherent. A management application is used to provide this access for simplicity.

All requirements were met, even though the perceived usage of them was not defined in scope (such as with the Docker deployment). This allows for future flexibility and although functionality is there, it is more of a future expansion placeholder. This is also the case with the cloud pod architecture, as resources for the VDCs are limited. There are images and templates in the vCloud Director catalogue to be deployed and will be functional when host resources increase. For the interim, if a VM requires predictable performance, it will run on a non-nested host.

1.4 Intended Audience

This document is meant for the key stakeholders in the project as well as technical staff leads required for a successful deployment.

1.5 Requirements

Below are the requirements as defined by the scenario document as well as additional communication with judges and creators in clarification emails.

1.5.1 Availability

Availability can be defined as “the proportion of the operating time in which an entity meets its in-service functional and performance requirements in its intended environment”. The criticality of the environment requires 100% availability as a service level objective (SLO).

Availability can be understood by understanding the relationship of Maintainability and Reliability. The chance a system will fail is based on Reliability. How quickly it can be fixed is due to it’s Maintainability. The combination of those two provide us with:

MTBF – Mean Time Between Failures (Reliability)

MTTR – Mean Time To Repair (Maintainability)

Availability is equal to MTTR/MTBF over the period evaluated.

R001	**Production systems require a “best effort” availability SLO**

1.5.2 Maintainability

Maintainability is defined as “the ability of an entity to facilitate its diagnosis and repair”. This is a key factor in availability.

R002	**The infrastructure must be quickly diagnosed and easily repaired**
R003	**The infrastructure must have a vCloud Director management component**
R004	**The infrastructure must be accessible in case of a total host failure.**

1.5.3 Integrity

System integrity is defined as “when an information system performs its function in an unimpaired manner, free from deliberate or inadvertent manipulation of the system”. In this context, it means that adds / moves / changes are not done on production systems.

R005	**The infrastructure must have adequate protection to avoid data loss**

1.5.4 Reliability

Reliability can be defined by having an absence of errors. Errors in a code base do occur, but there must be a method to ensure that they are tested, identified and resolved before they are put in production. This prevents the errors from affecting the overall application infrastructure.

In addition, infrastructure component configuration errors can cause reliability issues and faults. A method must be in place to ensure that all component configurations are correct.

R006	**A system must be in place to identify faults and areas of contention**

1.5.5 Scalability

Although the scope of the scalability has not been defined, the ability for it to occur with minimal additional design required.

R007	**The system must be scalable**

1.6 Constraints

C001	**The infrastructure must run on a single server with 16GB RAM**
	Memory is very limited and not all components can run simultaneously
C002	**There is only one uplink from the host**
	This is a single point of failure and makes nested network segmentation extremely difficult.
C003	**Docker must be implemented**
	Docker must be deployed, though no use case defined
C004	**vCloud Director must be deployed**
	vCloud Director must be deployed, though no use case defined

C005	**Only 250GB storage is available on DAS**
	There is no shared storage
C006	**There is no firewall**
	ESXi server is exposed to the internet. No routing in place for VMs
C007	**Infrastructure must be nested ESXi**
	This causes issues with networking
C008	**The system must be backed up**
	There is no shared storage in place for this

C009	**VXLAN must be implemented**
	Multiple clusters are required for this

1.7 Risks

R001	**Components may fail with no replacement available**

	System would be completely offline until replacement parts used.
R002	**NIC or uplink failure will make infrastructure un-available**
	The main ESXi host has a single NIC uplink
R003	**Resource constraints will make server non-functional**
	Some or all components may cease to function if adequate resources are not available.
R004	**Data loss may be unrecoverable**
	Lost data may never be recovered as there is now offsite replication
R005	**Staff may not have the skill to manage the environment**
	This may reduce the manageability of the environment.

1.8 Assumptions

A001	**The required staff will be available and have been trained to support the environment and work as a team.**
	The minimum required is 1 person and an offline Pluralsight library.
A002	**No additional hardware available**
	Once in space, there are no replacement parts unless they reside at the moonbase.
A003	**Adequate power is available**
	This includes clean power and multiple UPS battery banks
A004	**Additional hardware will be added in the future**
	This is to support the resource requirements of the modular components.
A005	**The environment will not use all components required until additional hardware is added**
	There are simply not enough resources to accommodate all components. Some VMs will not be run concurrently.
A006	**All equipment in this design is new and has been burn-in tested**
	A period of 1 week was used and all tests were passed without issue.
A007	**No zombies or zombie-like person will be onboard the shuttle or space-station**
	This includes poor Powerpoint presenters and people that get excited about scheduled meetings with no plan or agenda.

2. Architecture Design

2.1 Design Decisions

The architecture is described by a logical design, which is independent of hardware-specific details.

The following design decisions are presented with their justification.

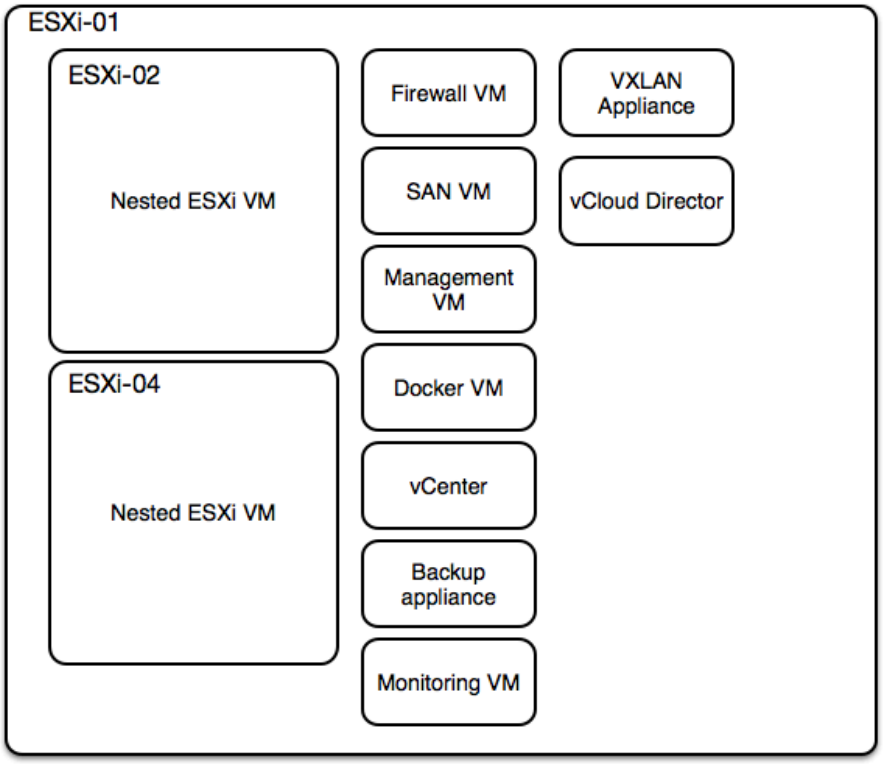
D001	**The system will have the fewest number of logical components possible**
	Complexity needs to be reduced to allow for easier maintainability and quicker diagnosis of issues.
D002	**Windows Server 2003R2 will be used for management, AD, DNS**
	With required roles and a responsive desktop, total RAM utilization is 200MB. This is the most efficient version that meets the requirements.
D003	**The appliance version of core components will be used.**
	This includes VCSA, vCloud Director, vShield Manager, VDP, vCOPS
D004	**Only portions of the infrastructure will run concurrently**
	This allows for a greater capability, as resources are available without additional configuration.
D005	**Windows 1.0 will be used to showcase the advanced features of "Reversi"**
	This meets the OS requirements with the smallest resource footprint of 4MB RAM.
D003	**Ubuntu LTS 14.x will be used as the Linux VM**
	This meets the defined guest OS requirements and has simple LXC / Docker integration
D004	**The vCloud Resource Group will have a Gold and a Silver Provider VDC**
	Each will have it's own dedicated cluster of compute.
D005	**A management compute cluster will be separate from the two compute clusters**
	Each cluster will only have one server because of resource constraints, but this sets the framework up for additional hardware later on.
D006	**Hardware version 10 will be used on the ESXi guests.**
	This allows it to pass hardware acceleration to the guest and run 64bit nested VMs
D005	**Promiscuous mode and forged transmits will be enabled on the physical host vSwitch0**
	This is required for proper nested ESXi host network communication

D006	Nested ESXi hosts will bridge the DVS uplinks to VSS port groups
	DVS port groups will have no VLANs, but VSS port groups will. This passing down the VLAN to the untagged DVS port groups

2.2 Conceptual Design

2.2.1 Nested Virtualization

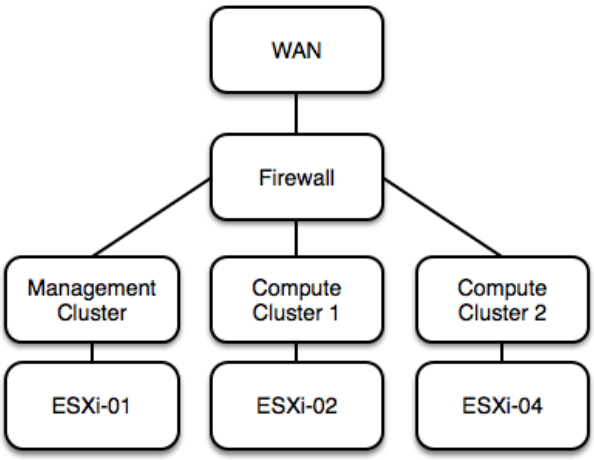
Below is the conceptual layout of the nested environment



Nested virtualization refers to the act of creating an additional layer of abstraction and encapsulation in a pre-existing virtualized environment. In nested virtualization, the differences in hypervisors, networking and storage in different clouds are abstracted, thus enabling existing virtual machines to be run on cascaded or third-party hypervisors and on other clouds without any modifications to the original virtual machines or their networking. This design makes use of ESXi inside ESXi.

2.2.2 Management Separation

If you put aside the fact that it is nested, it would look like this.



Separate management and resource clusters are important for the following reasons:

Separation of duties

A vCloud infrastructure typically has at least two types of administrator: infrastructure (vSphere) administrator and vCloud administrator. Separating the virtual management cluster from resource groups allows separation of duties and enforcement of administrative boundaries, limiting the actions that can be performed in the vSphere clusters of a resource group.

An administrator should not perform the following actions on a resource group through the vSphere Client:

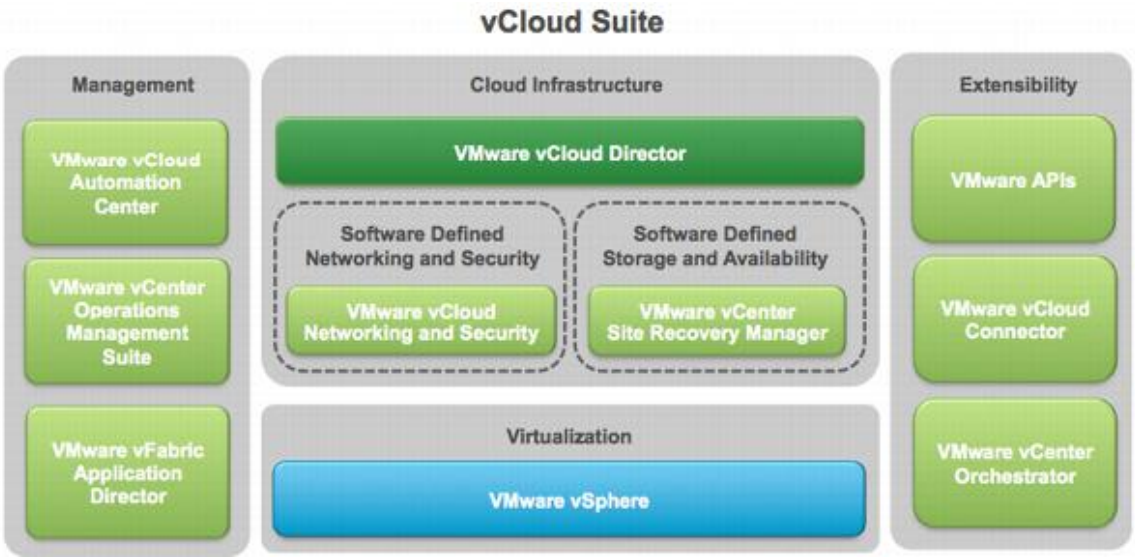
Editing virtual machine properties.
Renaming virtual machines.
Disabling VMware vSphere Distributed Resource Scheduler (DRS).
Deleting or renaming resource pools.
Changing networking properties.
Renaming datastores.
Changing or renaming folders.

This is not an exhaustive list, but it covers some of the detrimental actions a vCenter administrator could perform on a vCloud resource group.

2.2.3 vCloud Director Components

Below are the vCloud Director components:

Cloud Component	Description
VMware vSphere	Virtualization platform providing abstraction of physical infrastructure layer for vCloud. This includes: Sphere hosts. VMware vCenter Server. vCenter Server database.
VMware vShield Manager	Decouples network and security from the underlying physical network hardware through software-defined networking and security. This includes: VXLAN support. Cloud Networking and Security Edge gateway. Cloud Networking and Security App and vCloud Networking and Security Data Security. vCloud Networking and Security Manager.
VMware vCenter Operations Management Suite	Provides predictive capacity and performance planning, compliance and configuration management, dynamic resource metering, cost modeling, and report generation using the following components: vCenter Operations Manager. vCenter Configuration Manager. vCenter Infrastructure Navigator. vCenter Chargeback Manager.
VMware vCenter Orchestrator	Enables the automation of provisioning and operational tasks across VMware and third-party applications using an open and flexible plug-in architecture.



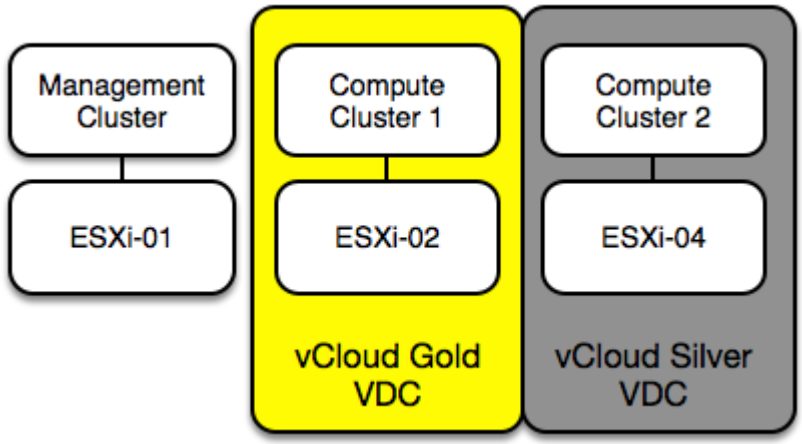
The following top-level logical building blocks are used to segregate resources that are allocated for management functions from resources dedicated to user-requested workloads.

vSphere virtual management cluster – Contains the core and optional components and services needed to run the vCloud instance. This includes core vCloud components such as VMware vCenter Server, vCloud Director, vCenter Chargeback Manager, vCenter Orchestrator, and optional components such as the vCenter Operations Management Suite

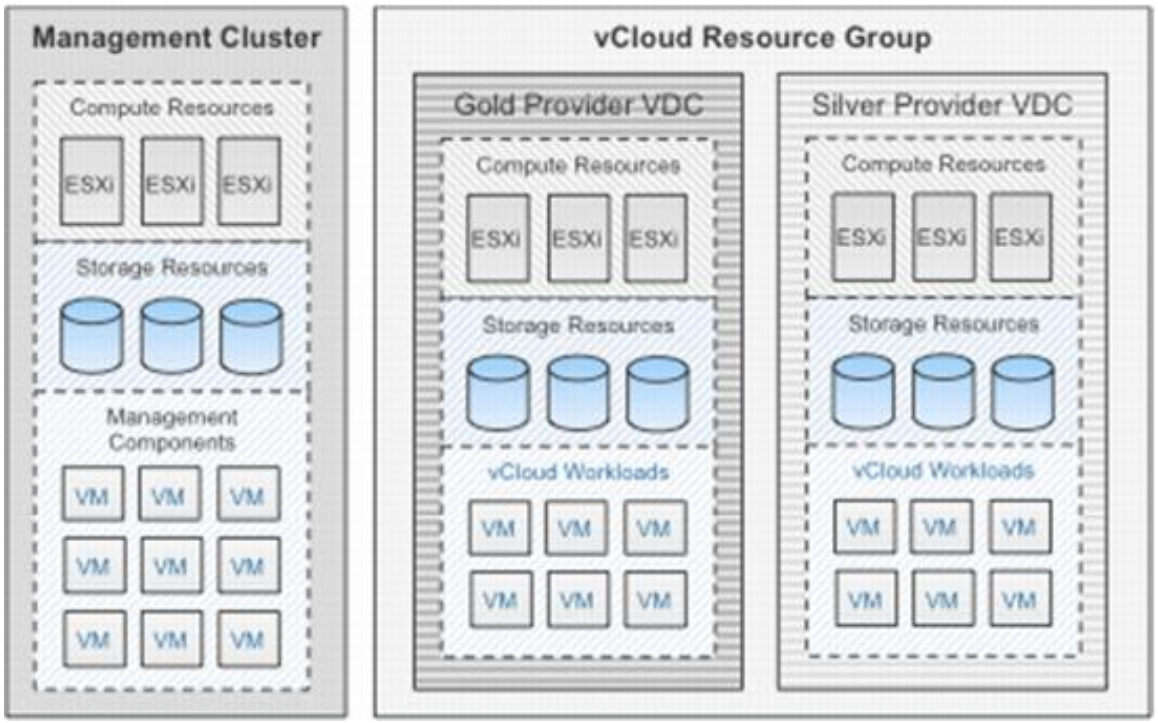
Resource group – Represents vCloud-dedicated resources for end-user consumption. Each resource group consists of vSphere clusters (vSphere hosts managed by a vCenter Server) and is under the control of vCloud Director. vCloud Director can manage the resources of multiple resource groups

2.2.4 vCloud Resource Groups

Below is the current vCloud model with the available resources we have in place.



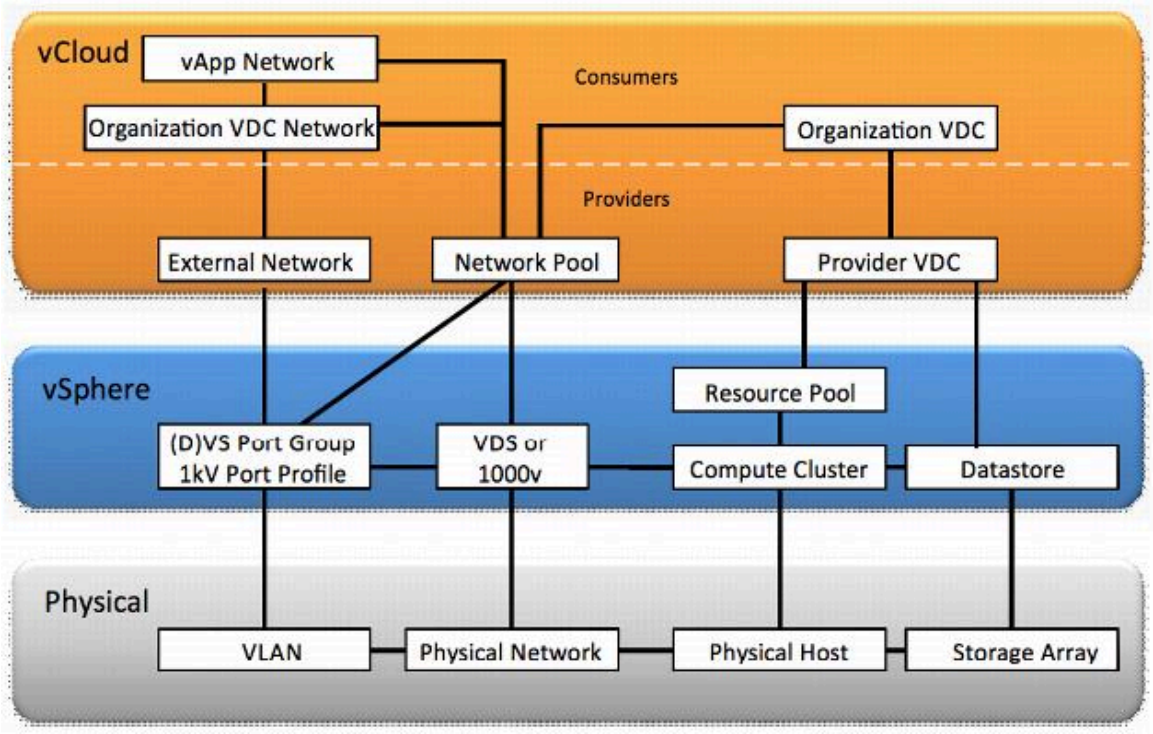
Below is an ideal model that will be achieved once more hardware is procured on the moon.



2.2.5 vCloud Director Constructs

vCloud Director introduces logical constructs to facilitate multitenancy and provide interoperability between vCloud instances built to the vCloud API standard.

The following figure shows the abstraction mapping for vCloud Director.



The following table describes the logical constructs for vCloud Director.

vCloud Director Constructs

Construct	Definition
Organization	The unit of multitenancy that represents a single logical security boundary. An organization contains users, virtual datacenters, and networks.
Provider virtual datacenter	A grouping of compute and storage resources from a single vCenter Server. A provider virtual datacenter consists of a single resource pool and one or more datastores. Multiple organizations can share provider virtual datacenter resources.
Organization virtual datacenter	A sub-grouping of compute and storage resources allocated from a provider virtual datacenter and assigned to a single organization. A virtual datacenter is a deployment environment where vApps can be instantiated, deployed, and powered on. An organization virtual datacenter allocates resources using one of the following models: ʾay As You Go. ʁeservation Pool. ıllocation Pool.
Catalog	A repository of vApp templates and media available to users for deployment. Catalogs can be published to all organizations in the same vCloud environment.
vApp	A container for a software solution in the vCloud, and the standard unit of deployment for workloads in vCloud Director. vApps contain one or more virtual machines, have power-on operations, and can be imported or exported as an OVF.
External network	External networks provide external connectivity to organization virtual datacenter networks

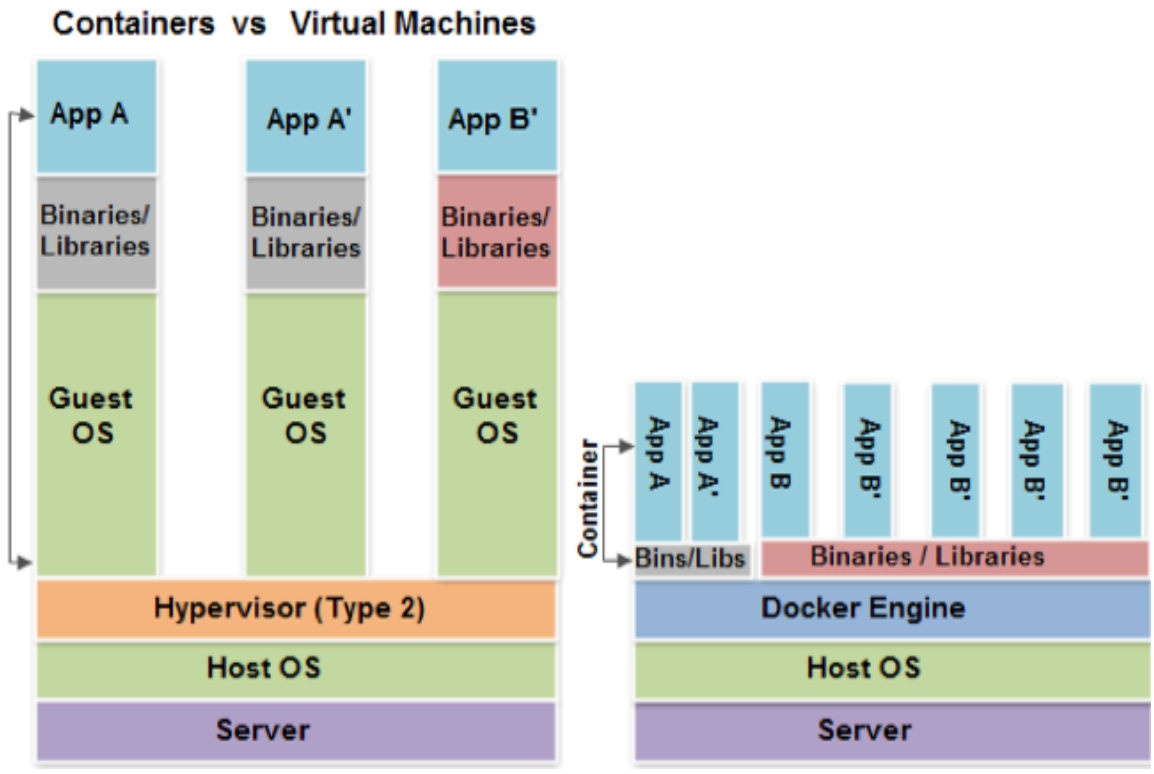
	and are backed by port groups configured for Internet accessibility.
Organization virtual datacenter network	Organization virtual datacenter networks are instantiated through network pools and bound to a single organization. Organization virtual datacenter networks map to a vSphere port group and can be isolated, routed, or directly connected to an external network.
vApp network	A network that connects virtual machines within a vApp, deployed by a consumer from a network pool. vApp networks can be directly connected or routed to an organization virtual datacenter network.
Network pool	A network pool is a collection of isolated Layer 2 virtual networks available to vCloud Director for the automated deployment of private and NAT-routed networks.

2.2.6 Docker Overview

LXC (LinuX Containers) is an operating system–level virtualization method for running multiple isolated Linux systems (containers) on a single control host.

Docker is an open-source project that automates the deployment of applications inside software containers, providing that way an additional layer of abstraction and automatization of operating system–level virtualization on Linux.

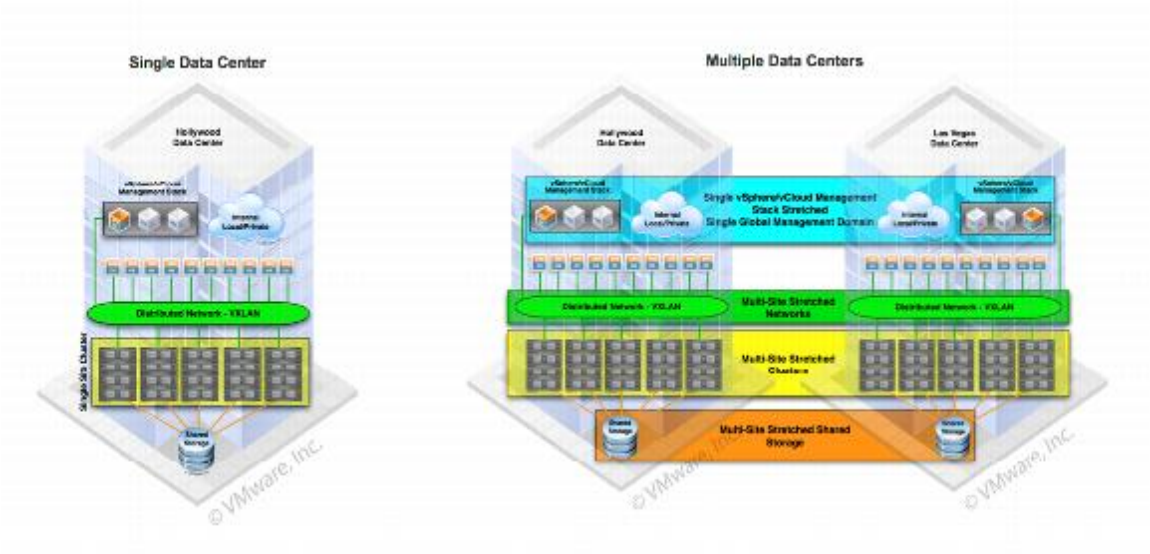
Here is the Docker (Linux containers) vs VM architecture comparison



Using Docker to create and manage containers makes it easier to create highly distributed systems by allowing multiple applications, worker tasks, and other processes to run autonomously on a single physical machine or across a spectrum of virtual machines. This enables the deployment of nodes as resources are available or needed

2.2.7 VXLAN Overview

Virtual Extensible LAN (VXLAN) is a technology that enables the expansion of isolated vCloud architectures across Layer 2 domains beyond the limits imposed by the IEEE 802.1Q standard. By using a new MAC-in-UDP encapsulation technique, a VXLAN ID adds a 24-bit identifier, which allows networks to push beyond the IEEE 802.1Q limit to a possible 16 million logical networks.



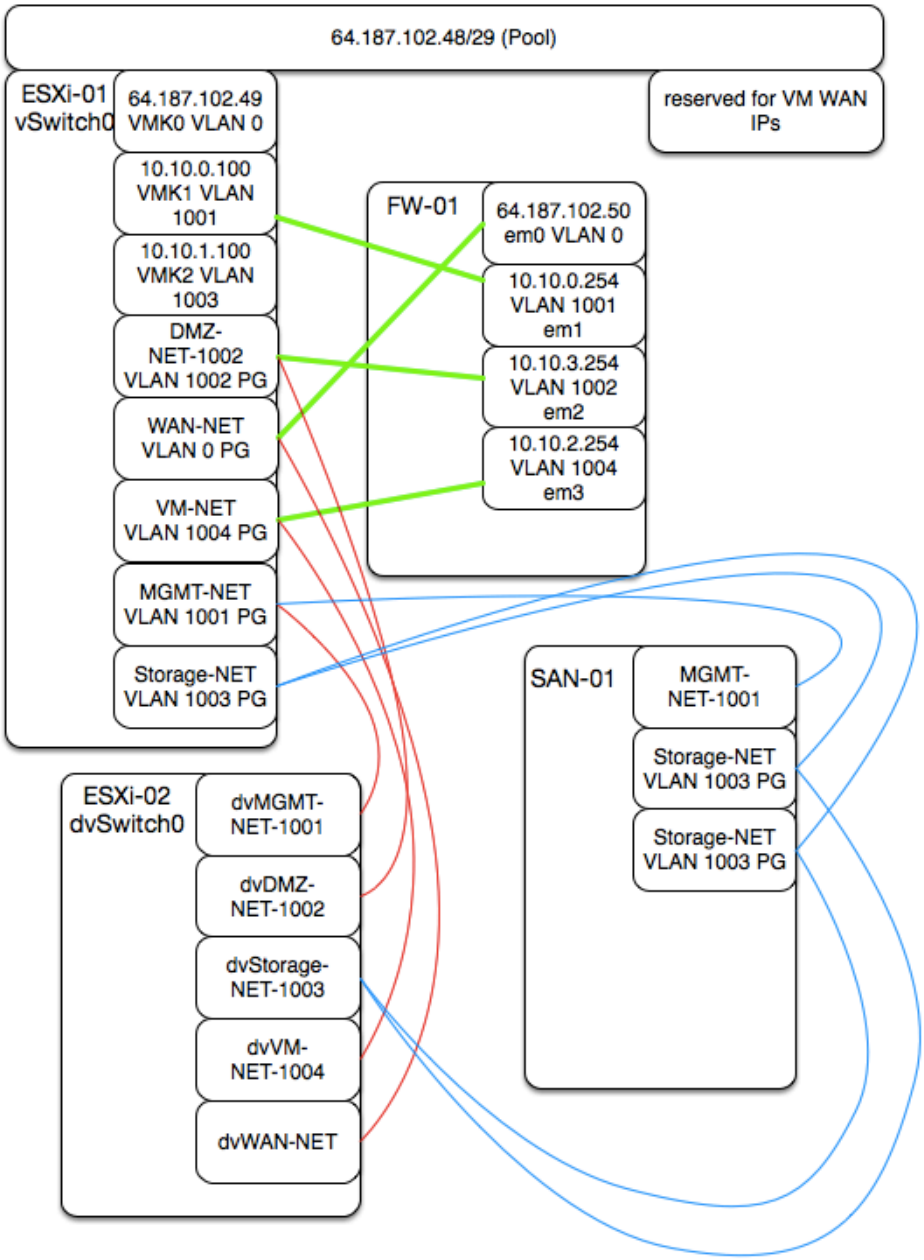
A virtual wire has been created between COMPUTE-Cluster-1 and COMPUTE-Cluster-2. The VMs associated with it are LIN-01 and LIN-02. This network is PoC only and serves no further purpose.

2.3 Logical Design

The Logical Design provides a more detailed view of the Conceptual Design components to meet the requirements. The architecture building blocks are defined without the mapping of specific technologies.

Below is the logical design for the core network of the infrastructure. This shows the VLANs and VM association.

2.3.1 Logical Network Design



2.3.2 Network IP Addressing

VLAN	Description
0	WAN connectivity
1001	Management
1002	DMZ
1003	Storage
1004	VM Networks

Hostname	IP	VLAN	Description
FW-01	64.187.102.49	0	Public facing firewall interface
ESXi-01	10.10.0.100	1001	Management VMkernel
ESXi-02	10.10.0.101	1001	Management VMkernel
ESXi-04	10.10.0.103	1001	Management VMkernel
FW-01	10.10.0.254	1001	Management facing firewall interface
MGMT-01	10.10.0.50	1001	Domain Controller
VC-01	10.10.0.99	1001	vCenter
SAN-01	10.10.0.200	1001	SAN management interface
VCD	10.10.0.20	1001	vCloud Director management
VSM	10.10.0.250	1001	vShield Manager
VDP	10.10.0.30	1001	VMware Data Protection
LIN-03	10.10.0.14	1001	Docker VM
AVM	10.10.0.32	1001	vCOPs Analytics VM
UIVM	10.10.0.33	1001	vCOPS UI VM
FW-01	10.10.3.254	1002	DMZ facing firewall interface
SAN-01	10.10.1.200	1003	SAN iSCSI Target
SAN-01	10.10.1.201	1003	SAN iSCSI Target
ESXi-01	10.10.1.100	1003	iSCSI VMkernel
ESXi-02	10.10.1.101	1003	iSCSI VMKernel
ESXi-02	10.10.1.111	1003	iSCSI VMKernel
ESXi-04	10.10.1.103	1003	iSCSI VMKernel
ESXi-04	10.10.1.113	1003	iSCSI VMKernel
FW-01	10.10.2.254	1004	VM facing firewall interface

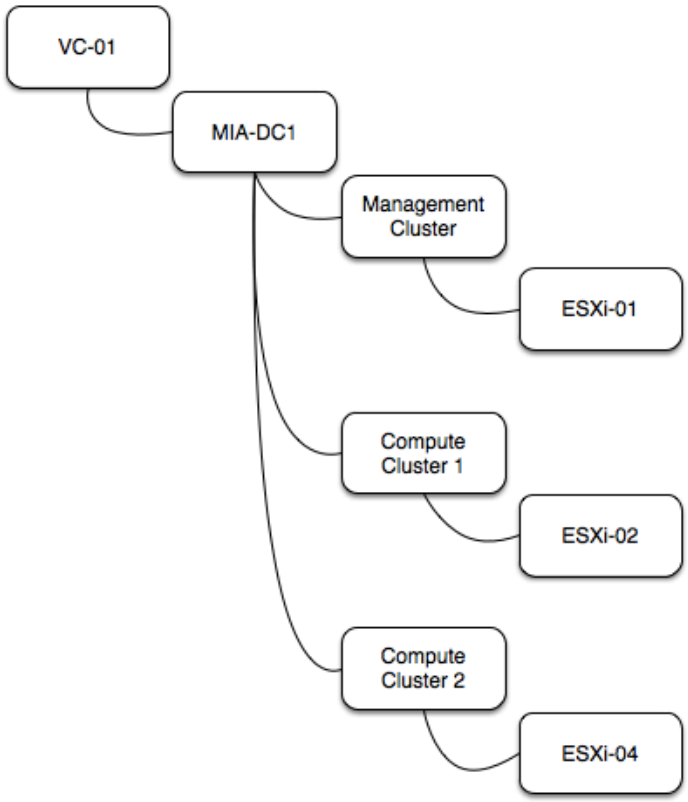
2.3.3 Login credentials and locations

Address	User	Pass	Description
10.10.0.99	administrator@vsphere.local	vdmchallenge	vCenter Server
https://Vc-01.zombie.local:9943/vsphere-client	administrator@vsphere.local	vdmchallenge	vCenter Server
10.10.0.100	Root	vdmchallenge	Management VMkernel
10.10.0.101	Root	vdmchallenge	Management VMkernel
10.10.0.103	Root	vdmchallenge	Management VMkernel
https://10.10.0.20/cloud/	Admin	vdmchallenge	VCD login
https://10.10.0.250	Admin	vdmchallenge	Domain Controller
10.10.0.30	Root	VDMchall1	VMware Data Protection Appliance
https://10.10.0.250	Admin	vdmchallenge	Domain Controller
10.10.0.30	Root	VDMchall1	VMware Data Protection Appliance
10.10.0.33	admin	VDMchall1!	vCOPs
64.187.102.50	admin	VDMchall1!	vCOPs
https://199.16.200.129	dracadmin	tP9H4rDH44G9!	iDRAC Management

2.3.3 vSphere cluster Logical Design

All management VMs will run in an HA/DRS clusters within vSphere. Management clusters are physically separated from compute clusters. Since we are limited on the actual number of hosts, the physical ESXi host ESXi-01 will be the sole member of this management cluster.

The compute cluster are also limited on resources, so they will have 2 cluster with 1 host each. This is the minimum number required for the framework of the environment. HA and DRS functions will not work, but resources pools can be created now in expectance of the addition of more in the future.



2.4 Physical Design

The physical design will be examined as a node in the blade chassis. The server being used for this at the time is the Dell M610 blade in the M1000 chassis. Only a single blade is used.

Feature PowerEdge M610 technical specification
Processors Quad-core or six-core Intel® Xeon® processors 5500 and 5600 series
Chipset Intel 5520
Memory1 x 16GB ECC DDR3 at 1333MHz
Drive bays Two 2.5” SAS/Solid State hot-swappable drives
Storage x 250GB
Hot-plug hard drive option

2.5 Virtualization Network Layer

2.5.1 High Level Network Design Network Segmentation and VLANs

There is a WAN network range of 64.187.102.48/29 provided to the infrastructure. This gives us 5 usable IPs.

64.187.102.48 - network
64.187.102.49 – FW-01 IP
64.187.102.50 - unused
64.187.102.51 - unused
64.187.102.52 - unused
64.187.102.53 - unused
64.187.102.54 – WAN Gateway

VLAN 1011 – Management
VLAN 1020 – Storage Communication (data channel)
VLAN 1030 – vMotion
VLAN 2001-2999 – VM networks

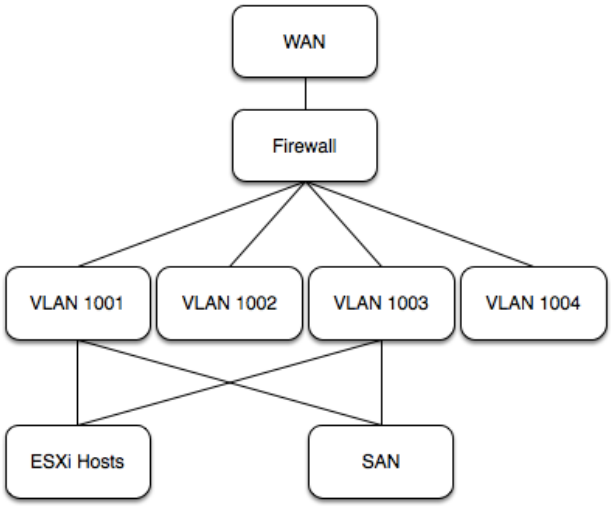
Out of band (OOB) communication will be done via the iDRAC which is at the following IP:

199.16.200.129

There is no direct access to the ESXi hosts or vCenter server from the internet. Port 3389 is open on IP 64.187.102.49 to allow for RDP access to the management server. From that server, access to the vCenter server and management VLAN (1001) is available.

This is in the interest of ease of access for reviewers, Upon completion of review, this port would be closed and remote access would only be available via a secure IPSEC VPN session.

Communication between VLANs is outward routed and firewalled hierarchically.



2.5.2 Virtual Standard Switches & Virtual Distributed Switches

There will be 2 vSwitches; a standard vSwitch for host ESXi-01 on and a distributed vSwitch only for all nested ESXi hosts.

The uplinks will be as follows:

vSwitch0 on ESXi-01 is a VSS. Uplinks are:

VNIC0

The following port groups are defined

MGMT-NET-1001 (VLAN 1001)
DMZ-NET-1002 (VLAN 1002)
STORAGE-NET-1003 (VLAN 1003)
VM-NET-1004 (VLAN 1004)
WAN-NET (VLAN 0)

The nested ESXi VMs have 10 VNICs, with 2 on each one of the VSS port groups. This allows for the definition of 2 uplinks per port group on each one of the distributed virtual switches.

dvSwitch0 on the nested ESXi hosts have the following uplinks. The associated port groups are also shown on the right. The teaming policy of the port groups specify only the specified VNICs in the table below.

Nested ESXi interface	DVS port group	Uplinked VSS port group
VNIC0	dvMGMT-NET-1001	MGMT-NET-1001
VNIC1	dvMGMT-NET-1001	MGMT-NET-1001
VNIC2	dvDMZ-NET-1002	DMZ-NET-1002
VNIC3	dvDMZ-NET-1002	DMZ-NET-1002
VNIC4	dvStorage-NET-1003	STORAGE-NET-1003
VNIC5	dvStorage-NET-1003	STORAGE-NET-1003
VNIC6	dvVM-NET-1004	VM-NET-1004
VNIC7	dvVM-NET-1004	VM-NET-1004
VNIC8	dvWAN-NET	WAN-NET
VNIC9	dvWAN-NET	WAN-NET

There are no VLANs defined in the DVS port groups, as they are inherited from the VSS port group uplinks.

Another model would have been to use fewer uplinks, but not pin them to any specific port groups. A port group on the VSS on ESXi-01 called “uplink” would have to be created as a trunk between physical and nested hosts. This would limited the nested bandwidth to the fewer uplinks. This model is “required” when there is more than 10 VLANs that need to communicate directly with the physical host or networks.

2.5.3 NIC Teaming

The uplinks on the DVS port groups have an active / active policy using the route based on originating port ID. This is the default policy.

2.5.4 Network I/O Control

NIOC will not be used as there is adequate separation on the DVS and only one 1GB uplink on the VSS (which also cannot make use of NIOC).

2.5.5 Physical Switches

The physical switches are abstracted and there is no visibility into them.

2.5.6 DNS and Naming Conventions

Domain will be zombie.local
Hostnames will be constructed by role, numerical ID and domain.

Example:
Role: ESXi server
Numeric ID: 01
Domain: zombie.local

FQDN: ESXi-01.zombie.local

2.6 ESXi Host Design

2.6.1 ESXi Host Hardware Requirements

The physical ESXi server will have:

2 sockets with intel E52600 series CPUs (8 core).
16GB RAM
2 x 250GB RAID1 drives
1 x 1Gbps NIC

The server is a blade in a Dell 1000 series chassis.

The nested ESXi server will have:

2 x socket with 1 vCPU each
4GB of RAM
4GB VMDK for local datastore
10 x VMXNET3 NICs

2.6.2 Virtual Data Center Design

There will be one data center named after the physical location. In this instance it is Miami, so the name is MIA-DC1.

2.6.3 vSphere Single Sign On

Single Sign-on will be used and the local LDAP domain @vsphere.local will be used.

2.6.4 vCenter Server and Database Systems (include vCenter Update Manager)

The vCenter Server Appliance (VCSA) will be used, as the total number of hosts is within the maximums. Update Manager will not be used due to the lack of updates being created, the limited number of hosts and extra resources required..

2.6.5 vCenter Server Database Design

The embedded database will be used for the vCenter server.

2.6.6 vCenter AutoDeploy

vCenter AutoDeploy will not be used.

2.6.7 Clusters and Resource Pools

There will be 3 clusters spanned across the 3 hosts. Resource pools will be managed by vCloud Director

2.6.8 Enhanced vMotion Compatibility

EVC will not be used at this time, as the number of hosts per cluster is 1.

2.6.9 Fault Tolerance (FT)

FT will not be used.

2.7 DRS Clusters

DRS will be enabled and set to manual. This allows for vCloud Director to create resource pools and assign them as needed.

HA will be disabled as there is only one host per cluster.

2.7.2 Resource Pools

Only vCloud Director will create resource pools.

2.8 Management Layer Logical Design

2.8.1 vCenter Server Logical Design

The vCenter server will be on the VCSA with 4GB of RAM allocated to support all the hosts. It will reside on ESXi-01 as a critical VM.

2.8.2 Management and Monitoring

vCenter Operations Manager will be used to monitor the environment in detail.

Due to resource constraints the vCOPS vAPP will not be turned on until more memory or hosts are available.

2.9 Virtual Machine Design

2.9.1 Virtual Machine Design Considerations

Operating systems will be comprised of a system volume and one or more data volumes. System volumes will not be larger than 100GB in size and will be thin provisioned by default.

Swap files for all VMs will be located on a swap datastore.
No RDMs will be used.
Virtual Hardware Version 10 will be used by default.
All operating systems that support VMXNET3 will use it as the network adapter of choice.

For this PoC environment, there will only be one virtual disk per VM with the minimum possible space allocated.

2.9.2 Guest Operating System Considerations

The windows VMs will have the version with the lowest resource requirements that meet the role requirements. AD will be on a Windows 2003 server, PoC guest will be on a Windows 1.0 workstation.

The Docker VM, which is considered a non-critical “core” VM will run on ESXi-01 and have the latest version of Ubuntu LTS, as it has tight LXC / Docker integration.

2.9.3 General Management Design Guidelines

Authorized personnel only will do all management of the environment, from a dedicated VM named MGMT-01.

2.9.4 Host Management Considerations

The physical server has a built in IP KVM in it’s management framework. This will require ActiveX or Java from the client machine.

2.9.5 vCenter Server Users and Groups

User and groups will be created and managed by vCloud Director. Global administrators will be created manually using the internal LDAP server.

2.9.6 Management Cluster

MGMT-Cluster will be the management cluster. All VMs for management purposes, whether virtual infrastructure, storage or otherwise, will run on it.

2.9.7 Management Server Redundancy

vCenter server is normally protected by HA across the a cluster. However, due to the lack of resources, there is no redundancy.

2.9.8 Templates

All virtual machines will be spawned from a master image in a catalog in vCloud Director. There is also an ISO folder on the SAN datastore. OVF files to be deployed are held on the MGMT-01.

2.9.9 Updating Hosts, Virtual Machines, and Virtual Appliances

Updates will be done manually via the ESXCLI. VMs will make use of snapshots before hand and ESXi-01 will make use of hosting provider imaging.

2.9.10 Time Synchronization

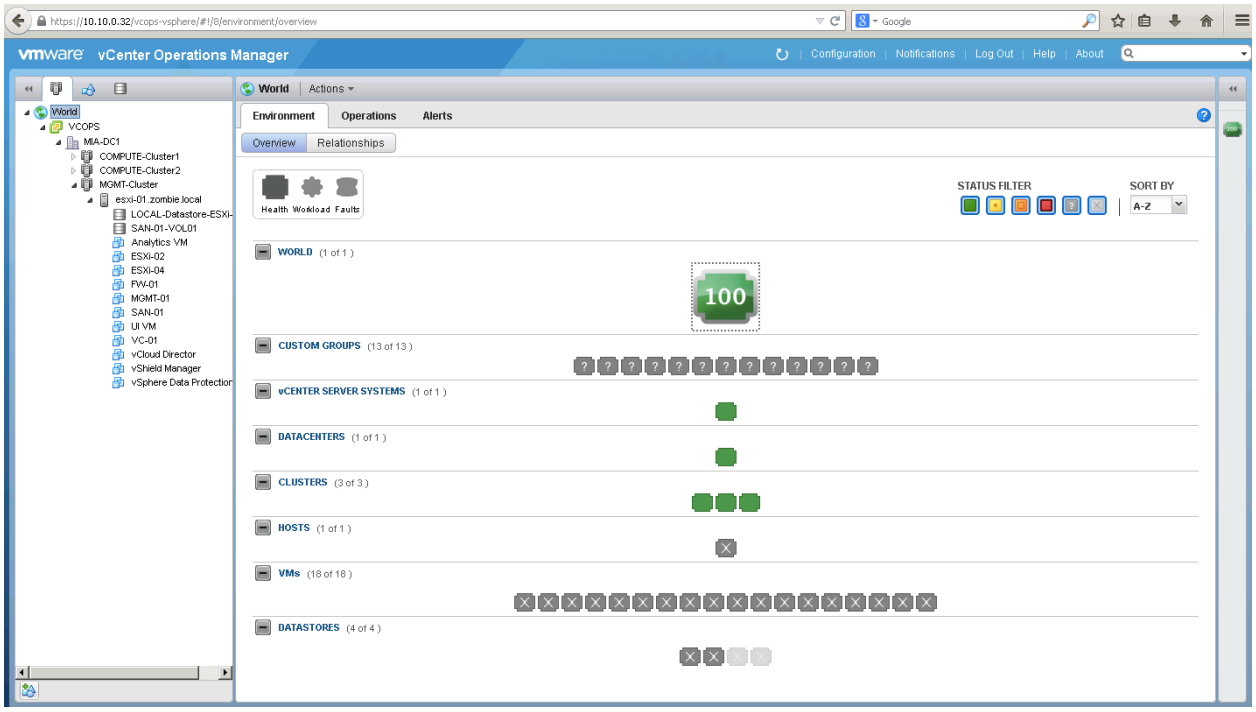
A GPS synced time server will be used for accurate time measurement. All hosts will connect to that NTP server. Active Directory VMs will be set to obtain the time of their hosts, then provide it to network computers.

2.9.11 Snapshot Management

VM snapshots will only be used before an add/move/change process to ease rollback if required. No SAN snapshots will be used.

2.10.1 Performance Monitoring

Performance monitoring will be done by vCOPs. See below for a screenshot of the deployment.



2.10.2 Alarms

All default vCenter alarms are enabled and the recipient is set to an internal email user.

2.10.3 Logging Design Considerations

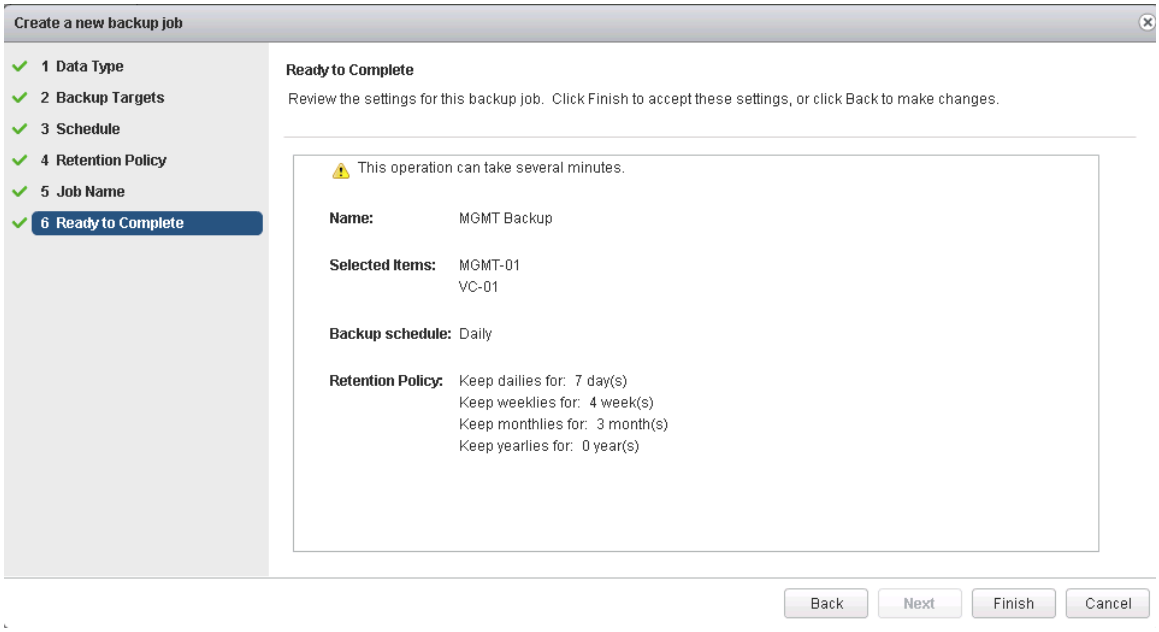
Log insight will be deployed, as more resources are available. Host logs will use a shared datastore on the SAN volume for centralization.

2.11 Infrastructure Backup and Restore

2.11.1 Compute (ESXi) Host Backup and Restore

Host configuration will be maintain in a single host profile and backed up with a PowerCli script. VMware Data protection will backup all VMs and appliances. ESXi-01 will be imaged regularly via the Clonzilla imaging solution of the provider.

Below is a screenshot of the retention policy for the management backup.



2.11.2 vSphere Replication

vSphere replication will not be used, at this time.

2.11.3 vSphere Distributed Switch Backup and Restore

The VDS config will be backed up as a function of the vCenter backup.

2.11.4 vCenter Databases

vCenter uses the internal VCSA database.