VIRTUAL DESIGN MASTER 3

TSETSE SWARM DESIGN DOCUMENT V1.10

Challenge 5

Steven Viljoen
8-1-2015

Contents

Revision History

Date	Revision number	Author	Comments
1 August 2015	V1.0	S.Viljoen	Initial draft
2 August 2015	v1.1	S.Viljoen	Mellissa, Mellissa, Mellissa….tsk,tsk,tsk
4 August 2015	v1.2	S.Viljoen	So no shared storage either…scratch that idea. (Thanks Eric)
4 August 2015	v1.3	S.Viljoen	Initial draft (2)
6 August 2015	v1.4	S.Viljoen	Initial draft (3)
7 August 2015	v1.5, v1.6	S.Viljoen	Feel like I'm writing a novel.
8 August 2015	v1.7	S.Viljoen	Something, something networks
9 August 2015	v1.9	S.Viljoen	Screenshots in document and you need to change an initial setting….
10 August 2015	v1.10	S.Viljoen	Maybe I should publish this in .mobi format.

Executive summary

Our scientists have 'somehow' managed to develop an Anti-Zombie Virus while sitting on Mars some 225 million kilometers away from the nearest Zombie and despite the increasing suspicions that they had something to do with the initial break out, plans have been drawn up to implement a Zombie Assassination System.

This system would involve using drones on Earth to deploy the virus vials to selected zombie infested areas and then report back on the effect so that our scientist back on Mars can make adjustments to their formulas.

Chief Scout, Melissa, has been sent back to Earth at great expense to find the best possible hardware on which we can build a state of the art, global, public cloud infrastructure.

She failed!

Instead we will be building a multi-tenant private cloud spanning 2 sites that can support 2 small workloads. (And even that is a stretch).

To prove that our systems are capable we will need to deploy these 2 workloads using an orchestration tool that we can fit on these ~~calculators~~ servers.

We will need to create an overlay network and plan from resiliency given that the servers have only a single NIC each and no shared storage.

Requirements

Reference	Description
RQ001	Applications must have multiple layers of resiliency.
RQ002	Infrastructure must support multiple tenants.
RQ003	Must run at least 2 workloads. (This might actually be better under risks)
RQ004	Must use some orchestration tool to deploy workloads.
RQ005	Should provide for future expansion.

Constraints

Reference	Description
CS001	Physical servers have already been procured.
CS002	Physical hosts only have 1 NIC each.
CS003	Physical hosts only have access to a single local disk each which can be used. *(Eric's orders! Think he spends too much time hanging around Melissa.)*
CS004	Physical hosts only have 12GB RAM each.
CS005	Only 2 physical hosts are available.(One per site)
CS006	Server 1 in Site A only has a single 120GB local disk.

Risks

(a.k.a. You name it, we've got it)

Reference	Description
RI001	Failure of a single physical NIC equates to a site failure.
RI002	Failure of the local storage equates to a site failure.
RI003	Failure of a physical host equates to a site failure.
RI004	No high availability across physical vSphere layer for the management VMs.

Assumptions

Reference	Description
AS001	With all surviving humans having fled the Earth, Zombies have adapted their diet to include any server more powerful than a calculator and these 2 were all that is left.
AS002	A small group of dedicated IT professionals out there will still be releasing patches and updates for the software we are using.
AS003	The servers have electricity.

Physical Layout

Physical servers have been specially [1] chosen and provided to us. [CS001] [AS001]

Server 1

- Model: Dell M610
- CPU: 1 x 1x2.0 GHz Gainestown E5504
- Ram: 12GB DDR3-1333 [1]
- Hard drive: 1 x 120.0GB [1] 2.5" SATA 7200RPM
- 1 Network Interface [1]

Server 2

- Model: Dell M610
- CPU: 1 x 1x2.0 GHz Gainestown E5504
- Ram: 12GB DDR3-1333 [1]
- Hard drive: 1 x 500.0GB 2.5" SATA 5400RPM [1]
- 1 Network Interface [1]

Shared Storage: **None** [1]

[1] Note to any future apocalypse survivors: Mellissa is probably not your best candidate to go out and find suitable HW for you!!

Conceptual design

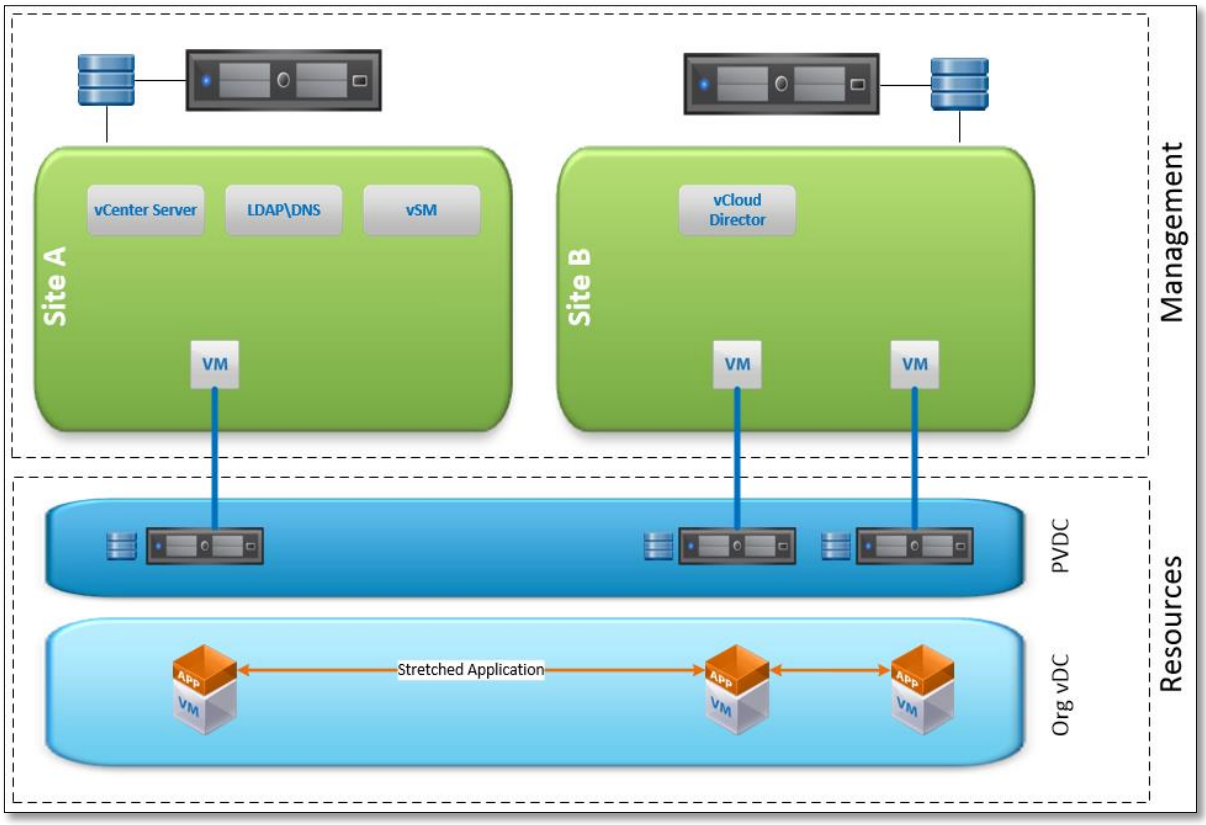
Overview

For this project I will be using vCloud Director to provide the multi-tenant cloud infrastructure with vShield Manager being used to create the VXLAN overlay network between both sites. vCO will be used for the automation of the environment.

Given the severe constraints on the physical layer it has been decided to focus on the application high availability [RQ001] by creating multiple layers of resiliency on the application layer.

To achieve this we have moved the cloud resource layer up to 3 virtual hosts (spanning both sites) each with their own local storage and will be using a stretched application approach as shown in the diagram below. (Why not present shared storage to the 2 virtual ESXi hosts in site B and use vSphere HA to protect the workloads locally you ask? See Design decisions below.)

This provides a quasi-Availability Zone approach allowing organizations the option to run their applications on either a single site, stretched across the 2 hosts in site B or stretched across both sites for high availability.



Application Resiliency

The following table illustrates the application resiliency options for specific site failures.

Physical site failures would be caused by any of the following:

- Physical NIC failure [RI001], Physical storage failure [RI002], Physical host failure [RI003]
- Actual site failure.

Failure Type	Stretched application impact	Single site application impact
Physical failure of site A	Organizational applications still accessible on Site B	Site A applications unavailable. Site B applications available.
Physical failure of site B	Organizational applications still accessible on Site A	Site A applications available. Site B applications unavailable.

Single virtual ESXi host failure: Site A.	Organizational applications still accessible on Site B	Site A applications unavailable. Site B applications available.
Single virtual ESXi host failure: Site B.	Organizational applications still accessible on Site A Organizational applications still accessible on Site B on the second virtual host.	Site A applications available. Site B applications available on the 2nd virtual host.
Two virtual ESXi host failure: Site B.	Organizational applications still accessible on Site A	Site A applications available. Site B applications unavailable.

Physical Layer Resiliency

Non-options

VSphere HA

- Given that there is no shared storage [CS003] it is not possible to use vSphere HA to protect the management virtual machines. [RI004]

VMware VSAN

- VSAN requires a minimum of 3 hosts presenting storage to the VSAN cluster so this is not possible. [CS005]
- VSAN requires at least 2 disks (1 flash & 1 capacity) which we don't have. [CS003]
- Even if there was an additional host, we would still be limited by the size of the VSAN shared disk given that physical server 1 only has 120GB local disk. [CS006]

Storage based replication

- As both physical hosts have access only to their individual local storage [CS003] this is not an option.

Hypervisor based replication

- Low RAM specs on the physical servers [CS004] prevent using hypervisor based replication options given that
  - Replication software would consume additional physical memory on each host.
  - A single physical hosts cannot run both sites management VM's memory workload without putting the organizational VMs and their applications at risk. [RQ001]

Local site backups

- Do not offer protection for site failures (in our case means a physical failure of any sort) [RI001] [RI002] [RI003]. Snapshot based backups would also cause Full Datastore issues in Site A.[CS006]

Cross site backups

- Given the size of Server 1 local storage [CS006] it is not possible to accommodate backups of the larger primary site (Server 2).

Workable option

While not a very pretty or standard solution the only real workable option left for us is to rebuild the infrastructure in case of failure. Given that the application should remain running in case of failures (as shown in the table above) the main point to focus on is how to streamline the build process in the background.

For this we will be implementing the following points:

- The build process for the infrastructure components will be fully documented so that it can be rebuilt again as quickly and as soon as possible.
- Any component configurations that can be exported to file will be exported and saved on both sites.
- All possibilities of scripting deployments will be used. Scripts will be stored on both sites.
- Emphasis will be placed on increasing the resiliency as soon as possible. See Future planning section.

Design Choices

DN001: VCenter server

The installable vCenter 5.5 server was chosen over the vCenter Server appliance for the following reasons.

- VCSA requires that VUM be installed on a separate VM thus consuming additional resources.
- Our IT specialist team (me) have more technical experience with Windows than Linux so makes it easier to configure and troubleshoot if needed.
- vCenter installable offers options that while not used in this design might be needed in the future:
    - IPv6 support
    - Powercli integration
    - vCenter heartbeat
    - vCenter linked mode

To further reduce the resource demand of the vCenter Server the Java memory settings have been limited.

DN002: ESXi servers

Given that there is only 1 physical NIC per server it is not possible to move both physical hosts to a Virtual Distributed Switch. The host containing the vCenter will always become disconnected from the vCenter at some stage of the migration and force a rollback.

(If anyone knows a way to migrate a single NIC host on which the vCenter server is running (and cannot be vMotioned as there is no shared storage) to a vDS I would really be glad to hear from you as I have tried a number of ways without success and the curiosity is driving me crazy ☺)

As a vDS is a requirement for vCloud Director the option was to either use only 1 physical host for the vCD Resource Pod or move the cloud layer up onto Virtual ESXi hosts that would allow resources to be spread across 2 sites instead of only 1.

DN003: Virtual ESXi storage

Local (yes, non-shared) storage has been presented to all 3 virtual ESXi hosts. *(You can stop laughing now, please)*

Presenting shared storage via software (NFS) to the 2 virtual ESXi hosts in Site B would create a single point of failure (i.e. The NFS server presenting the shared storage fails) that would negate the purpose of having 2 virtual ESXi hosts.

As the applications will in any case be stretched across virtual hosts it is better from a high availability aspect to have them running on their own standalone local storage.

DN004: VCloud Director Appliance

VCloud Director Appliance was chosen as it presents a smaller compute footprint (vCD appliance) as compared to vCAC which requires an Identity appliance, a vCAC appliance and an additional windows server for the IaaS components.

Yes, it's end of life in Q3 2017, but given the whole Zombie Apocalypse I doubt there is much of a VMware support team manning the phones even now, so probably not that much of a concern to us.

And yes, the appliance is limited to only 2 vCenters, 10 Organization vDCs and 100 Virtual machines, but that is more than the current HW could support in any case. See Future planning for scaling options.

It is also something that the IT specialist team (me again) have at least seen at some point in their life as opposed to vCAC or other options.

DN005: Single vCenter vCD setup

Normal vCloud deployments would use a 2 vCenter setup, with one vCenter used for the Management resources and 1 vCenter dedicated to the vCloud Resource pod. The main reasons for having 2 vCenters are:

- Limiting management domains.
    - VSphere admins can administer vSphere layer (Management pod) while vCD can manage the Cloud layer (Resource pod).
- Reduces stress and performance related issues on the management vCenter by offloading cloud tasks to the dedicated cloud vCenter.
- Keeps things separated and organised
    - VCloud Director basically creates organised chaos in an environment by adding a number of resource pools, portgroups, folders, etc which might not be understood by a lowly vSphere Admin and could lead to disaster

BUT….As we have very limited resources I have chosen to go with a single vCenter setup that will manage both the Management layer and the Resource layer.

HOWEVER….to mitigate some of the issues discussed above the Resource ESXi hosts have been added to a separate virtual Datacenter as opposed to simply another cluster within the Management virtual datacenter.

Reasons for doing this are:

- Limited Management domains can still be created by using role based access control on the Datacenter level so that only cloud admins and vCD have access to the Resource datacenter while vSphere admins have access to the management datacenter.
- As this is planned as a very small deployment (5 hosts in total) it is not expected that the vCenter will be placed under too much load. If needed an additional vCenter can be added to the vCloud Director appliance at a later stage. For further scaling possibilities see Future planning.
- As Virtual Distributed Switches are bound to virtual Datacenters.
    - An admin looking at the management datacenter will see only Management related distributed switches and the same applies to the resource datacenter which would show only the vCloud managed distributed switches.

DN006: DNS

While a DNS server has been configured in the environment it has been decided that IPs will be used instead of FQDNs.

While this goes against best practice the reason behind this decision is based on the fact that there is only 1 DNS server [CS004] which makes it is a single point of failure and as such the availability of the environment actually increases by using IP addresses.

The existing DNS server servers to future proof the environment.

Patching and Updates

Patching [AS002] in general will be handled as follows:

- Windows servers will be patched using WSUS offline to save on the resources of a dedicated WSUS server.
- VMware products will be patched using the VUM server installed on the vCenter Server.

Patching\Updating can be broken down into 3 main areas:

Virtual workloads

With the applications stretched across 3 virtual sites (Site A, Site B1, Site B2) patching and updating of the virtual workloads would be relatively simple as each sites' workload could be taken offline individually and patched while the other 2 remain online and available.

WSUS offline will be used to patch the Windows servers to save on physical compute resources that would be needed by fielding a WSUS Server on a separated VM.

Resource layer

In this sense this applies to the virtual ESXi hosts and the same reasoning applies as to the virtual workloads. Each virtual ESXi host (and its hosted workloads) could be taken offline individually for patching and\or updating while the other 2 remain online and thus ensuring that the stretched application remains available.

The VMware Update Manager installed on the vCenter will be used for patching the virtual ESXi hosts.

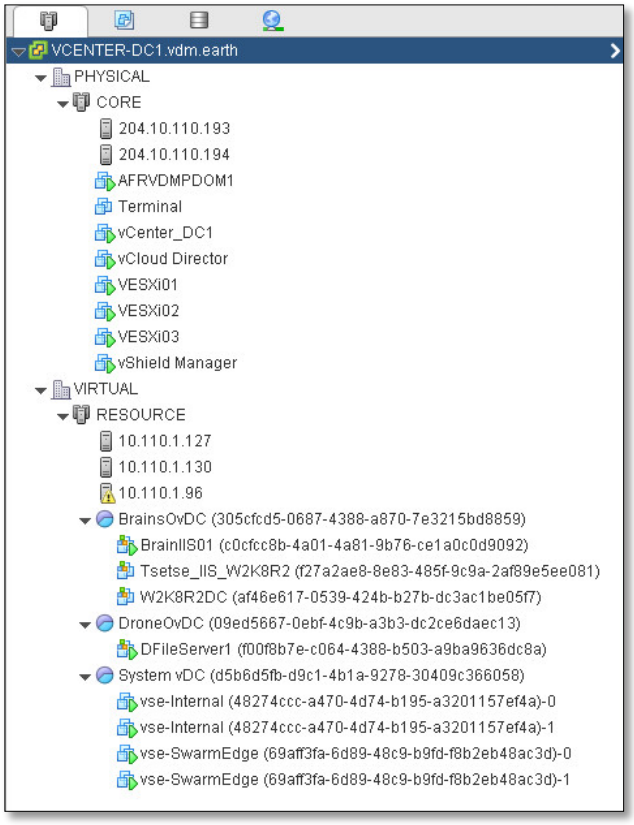
Management layer

The management layer includes all management components (vCenter, Domain Controller, vCD, vSM) and also the 2 physical ESXi hosts.

The following table describes the method and impact of patching each.

Component	Patching method	Impact
vCenter Server OS	WSUS offline	No impact to applications. No configuration changes can be made while vCenter is offline.
vCenter Server	upgrade	No impact to applications. No configuration changes can be made while vCenter is offline.
Domain Controller\DNS	WSUS offline	No impact to applications during short reboot after applying MS patches.
Site B: ESXi host 2	Patch using VUM.	Site B applications will be down. Site A applications will remain up.
Site A: ESXi host 1 (hosting the vCenter + VUM)	Not possible to place host into maintenance mode as vCenter server cannot be migrated. [CS003] A 'cold migration' of the vCenter server to the 2nd host will be needed. • Power down and remove vCenter from ESXi01 inventory. • Transport copy via USB. • Copy to ESXi02 and add to inventory. • Say a little pray and power it on. • Patch ESXi01 normally using VUM.	Site A applications will be down. Site B applications will remain up.

Logical design



Core Management Services

The following Virtual Machines make up the Core Management services per site

Name	Roles	vCPU	vRAM	HDD [1]
Terminal	Terminal Server			
AFRVDMPDOM1	Domain Controller for 'vdm.earth' domain. LDAP , DNS, NTP	2	2 GB	30 GB
VCENTER-DC1	vCenter Server & VUM Server	4	4 GB	40 GB
vShield Manager	vShield Manager	2	4 GB	60 GB
vCloud Director	vCloud Director	1	2.5 GB	30 GB
vESXi01	Virtual ESXi host 1 Site B	4	4 GB	200 GB
VESXi02	Virtual ESXi host 2 Site B	4	4 GB	200GB
VESXi03	Virtual ESXi host 2 Site A	4	4 GB	50 GB [2]

[1] All disks have been thin provisioned.

[2] *The usage of this scarce resource will be determined by a Hunger Games style management meeting which will be broadcast on Mars for the IT team's entertainment.*

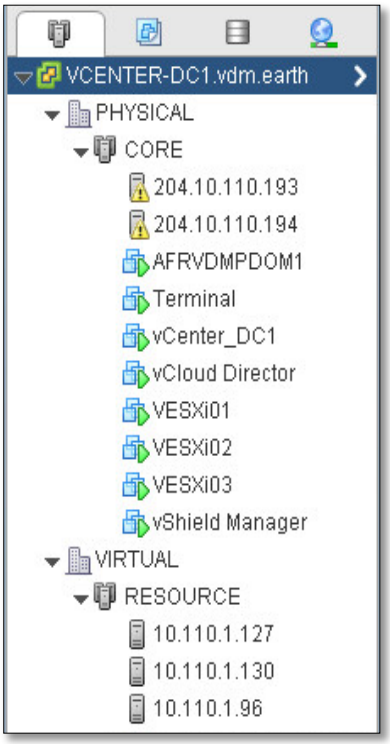
The Terminal server (highlighted above) was designed to be the single central entry point into the environment and while it has been deployed I have simply run out of time to get it up and running.

Virtual Datacenter layout

The environment consists of a single vCenter instance hosting 2 virtual datacenters [DN005] which are used to provide the management pod and the resource pod for the cloud environment.

PHYSICAL datacenter setup

- Single cluster (CORE)
- 2 Physical hosts have been added. [DN006]
- Hosts the Core management services VMs.
- vSphere HA and DRS are disabled [CS005]
- All networking is done via a single Standard Switch on both hosts.
    - VMkernel port
        - vMotion *(still optimistic about the future even after the last 6 weeks)*
        - Management traffic
    - VM Portgroup
        - Management VMs
        - Virtual ESXi hosts



VIRTUAL datacenter setup

- Single Cluster (RESOURCE)
- 3 Virtual ESXi hosts have been added. [DN006]
- Used for the tenant Virtual Machines.
- vSphere HA and DRS are disabled.

VCloud Design

The vCloud design is broken down into 2 sections:

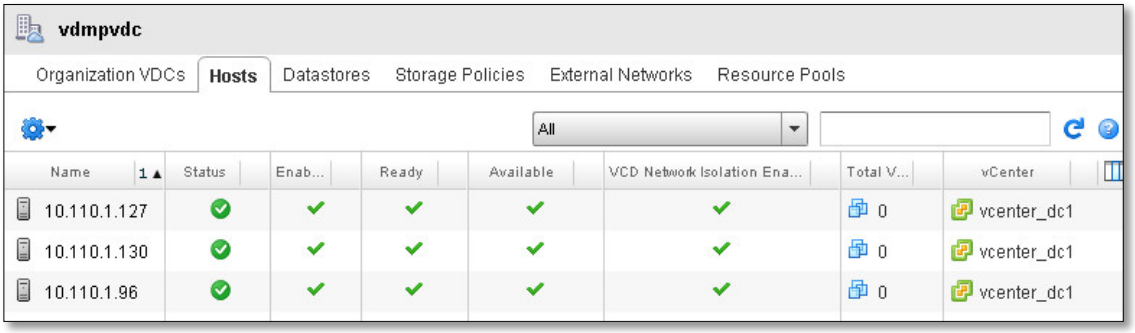
- **Provider virtual datacenter (PvDC)**
    - Combines and abstracts underlying the vSphere resources and makes these resource pools (compute, network & storage) available to the various organizations to use.
- **Organization virtual datacenter (OvDC)**
    - Created per organization.
    - Used to allocate resources from the PvDC resource pools to the specific organization.

Provider virtual Datacenter

A single PvDC (**vdmpvdc**) has been created using all the resources in the Resource cluster. (*See what I did there?*).

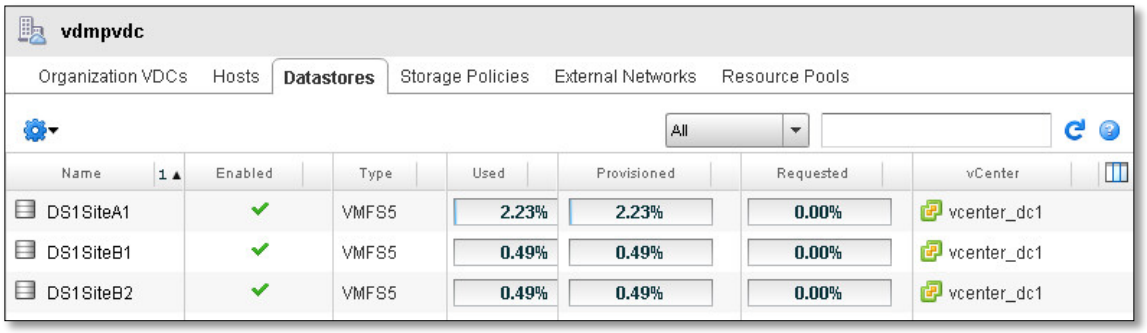
Hosts

All 3 virtual hosts have been prepared, enabled and are available in vdmpvdc.



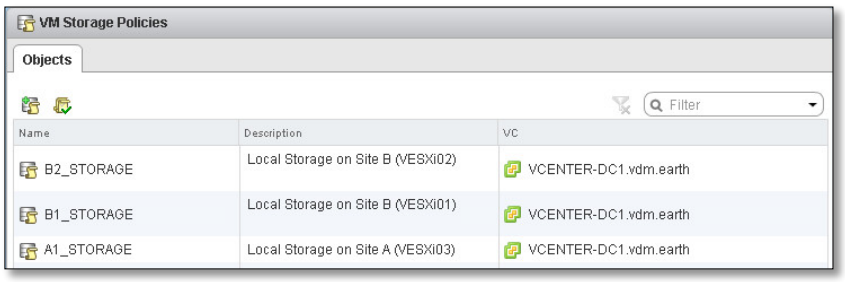
Datastores

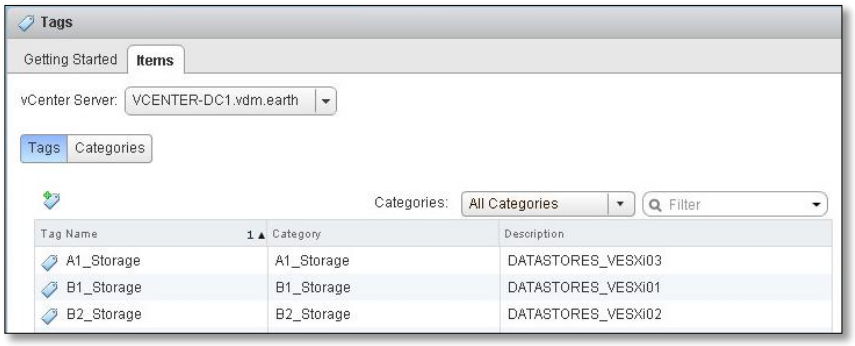
All 3 local datastores on the virtual ESXi hosts have been added (via Storage policies below) to vdmpvdc.



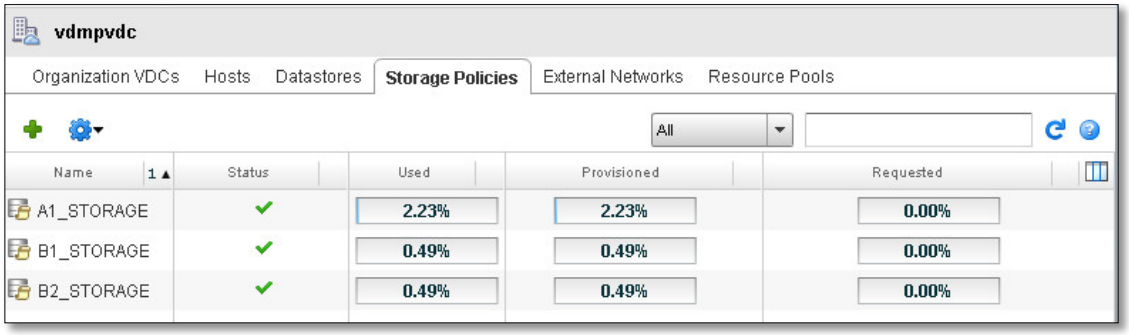
Storage policies

To simplify and ensure compliance, 3 separate Storage Policies have been created on the vSphere level to identify the specific site\host and mapped to custom Tags which are assigned to each of the individual local datastores.



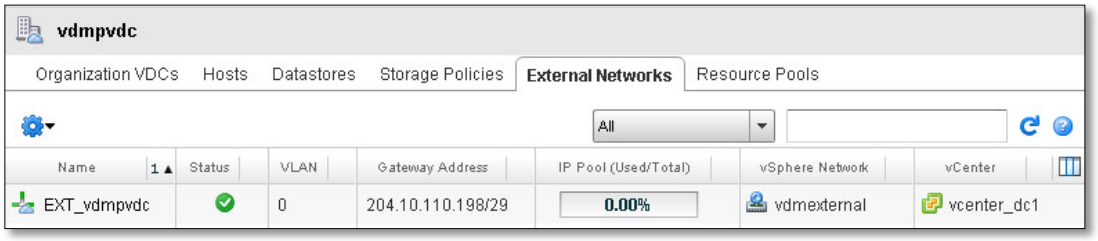


These have been allocated to the vdmpvdc PvDC.



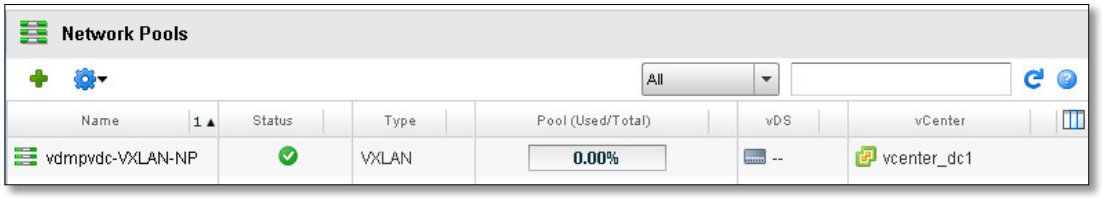
External Networks

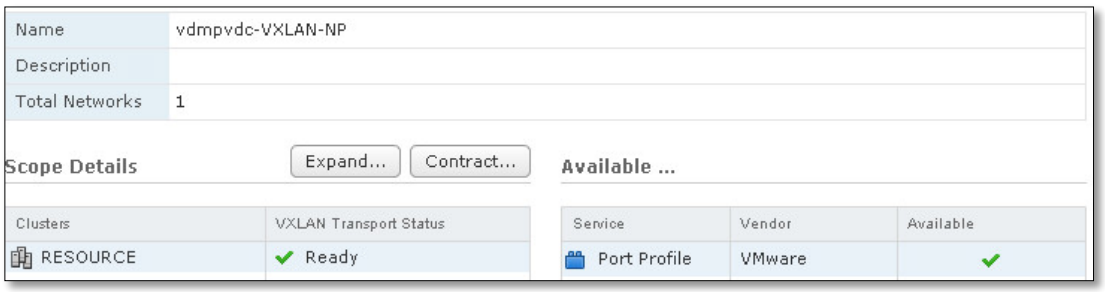
One external network has been created to allow the Organization VMs to communicate with what is left of the outside world and allocated to vdmpvdc with 1 static IP assigned. This is mapped to the 'vdmexternal' distributed portgroup.



Network Pools

A VXLAN type Network pool has been created to cover all hosts in the Resource Cluster.





Organization virtual Datacenter

For the Zombie Assassination System (ZAS) a new organization name TsetseSwarm [1] has been created.

([1]Tsetse is a large biting fly in middle Africa that is the main carrier of Human Sleeping disease parasitic disease and was the original idea behind using drones to deliver the ZAS vials-I'll wait while you Google fact check me.)

ZAS Overview

The program consists of two major parts.

Drones

- These will need to connect to a web based application to receive instructions as to which canister they should pick up and to where it needs to be deployed.
- They will also need to reconnect to the web upon completion to report mission status and upload their vial effect report.
- New frontend web applications will need to be deployed to spread the load as new drones come online.

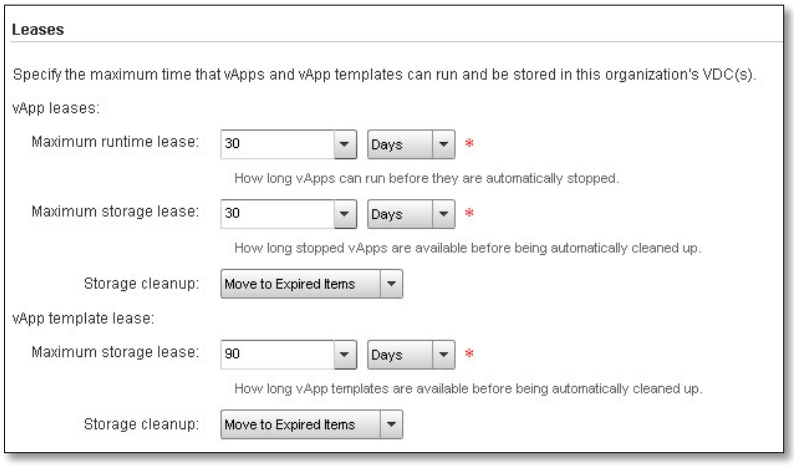
Scientists

- The scientists back on Mars will connect via a separate web application to analyze the effect report of each vial deployed by the drones.
- They will also need a web application by which they can enter instructions for the vial packing robots and upload new drone deployment instructions.

- Given the fact that there are a limited number of scientist (and probably a few less once they start mixing the chemicals) it is expected that their system requirements will be less dynamic.

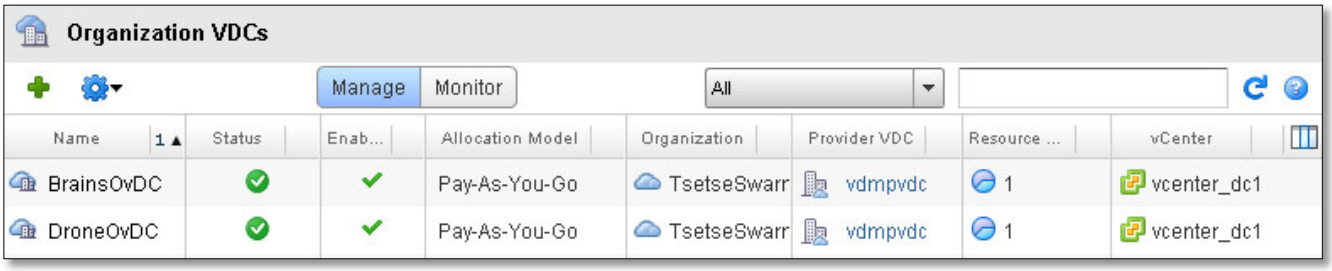
Tsetse Swarm Organization settings

- This organization will have 2 local users:
  - DroneAdmin Organization Administrator
  - BrainAdmin Organization Administrator
- Catalogs will NOT be allowed to be shared outside of the organization *(we were 'fortunate' enough to have an IT Security officer amongst the survivors)*
- Users will NOT be allowed to publish to external catalogs *(yip, him again)*
- Users will NOT be able to subscribe to external catalogs *(He seems depressed so we like humor him)*
- Leases
  - Given the low amount of resources available and the fact that drones might not return from missions and scientist might mix the wrong ingredients we have decided to limit the vAPP leases as follows:



- The organization specific URL created by vCloud Director for this organization is: https://10.110.1.103/cloud/org/tsetseswarm

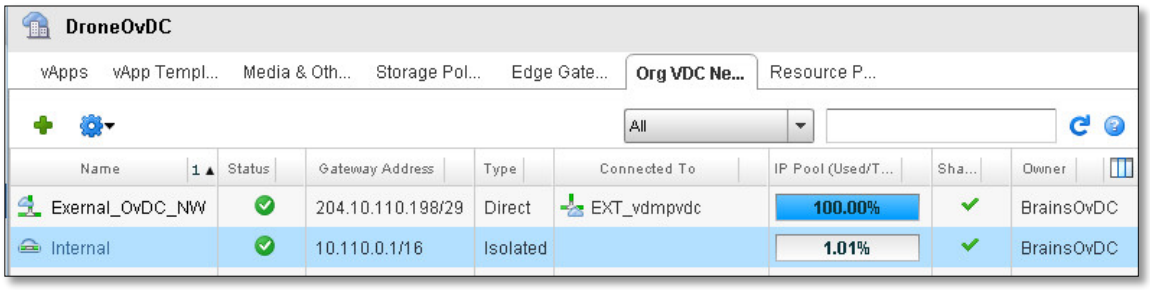
Based on this high level analysis, this organization will be assigned 2 Organization virtual Datacenters to ensure that each section of the program can manage its own resources, but can still make use of shared components.



Each OvDC will be configured with a Pay-As-You-Go allocation model as this model does not reserve any resources until a vAPP is deployed thus conserving our limited resources.

Organization Networks

2 Organization networks have been created and shared with both OrgvDCs.



External_OvDC_NW

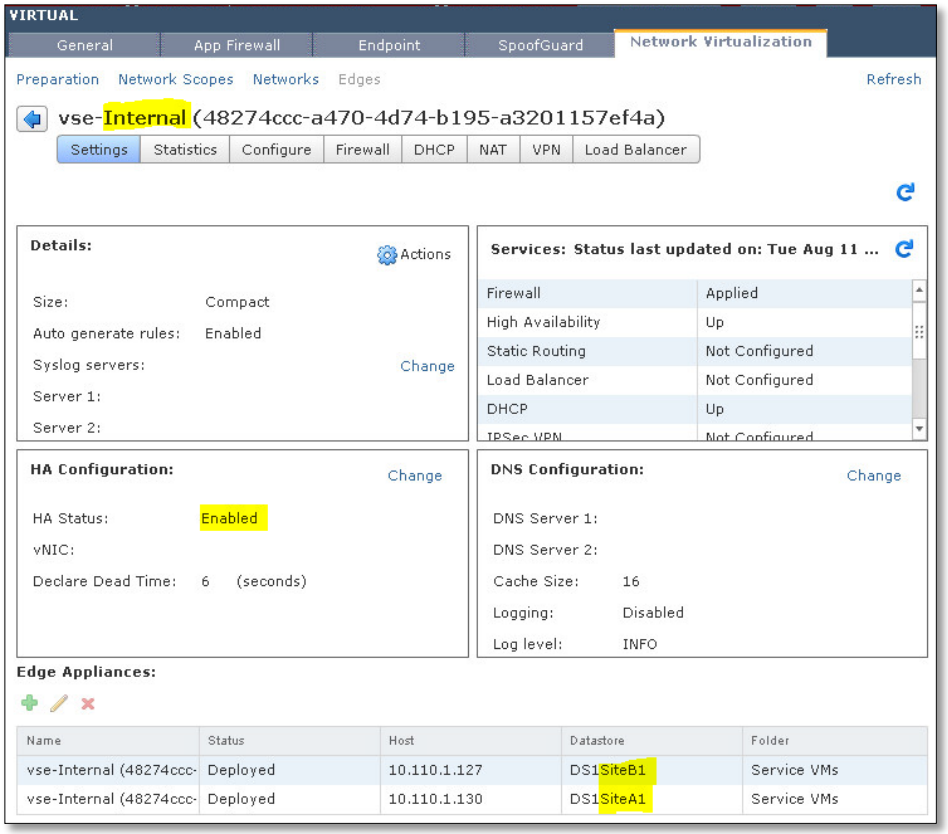
- A Direct External Network connected to EXT_vdmpvdc.
- Assigned a static IP pool consisting of 1 IP.

Internal

- An Internal isolated network
- Assigned a static IP pool consisting of 99 IPs (10.110.10.2 – 10.110.10.100)

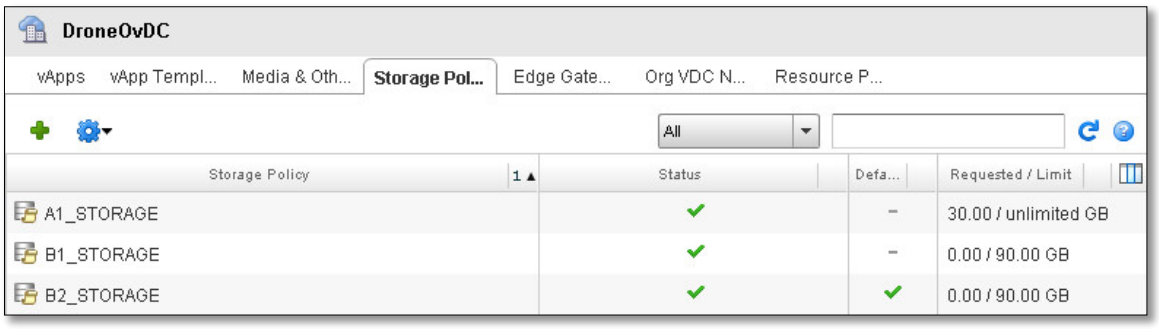
Edge Appliance

An edge has been deployed in a HA configuration with 1 appliance residing in Site A and the other in Site B.



DroneOvDC specific settings

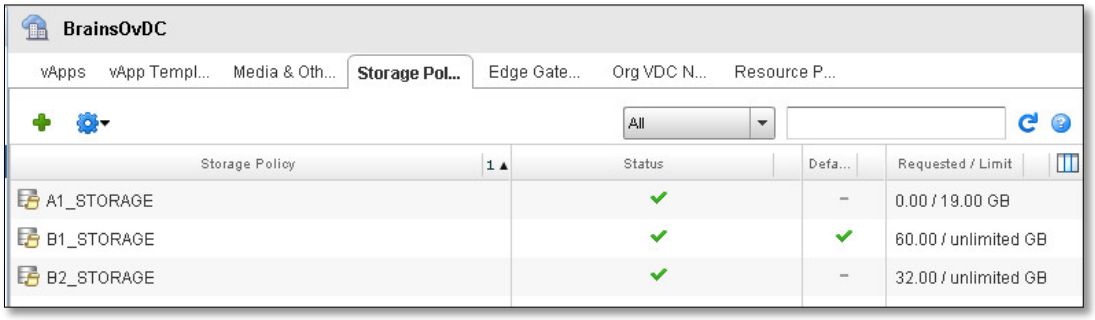
- Storage Policies
  - All 3 Storage policies have been assigned with limits set as shown below
    - A1_STORAGE limit has been set to unlimited given its small size.



- Org Networks
  - Both Org Networks listed above are available to the OrgvDC.

BrainsOvDC specific settings

- Storage Policies
  - All 3 Storage policies have been assigned with limits set as shown below
    - A1_STORAGE limit has been set to 19GB. *(Mostly just to mess with the scientists)*
    - The remaining 2 have been set to unlimited.
    - B1_STORAGE already shows 60GB requested.
      - This is space used by the 2 vApp templates in the catalog.

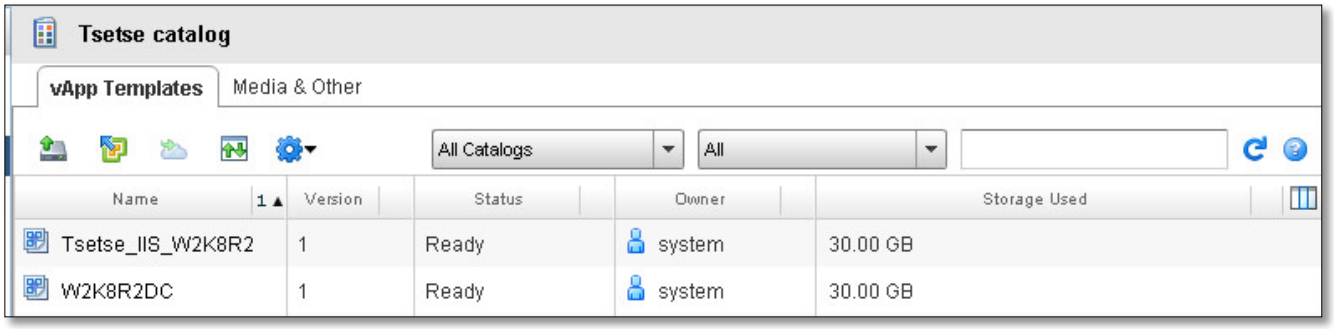


- Org Networks
  - Both Org Networks listed above are available to the OrgvDC.

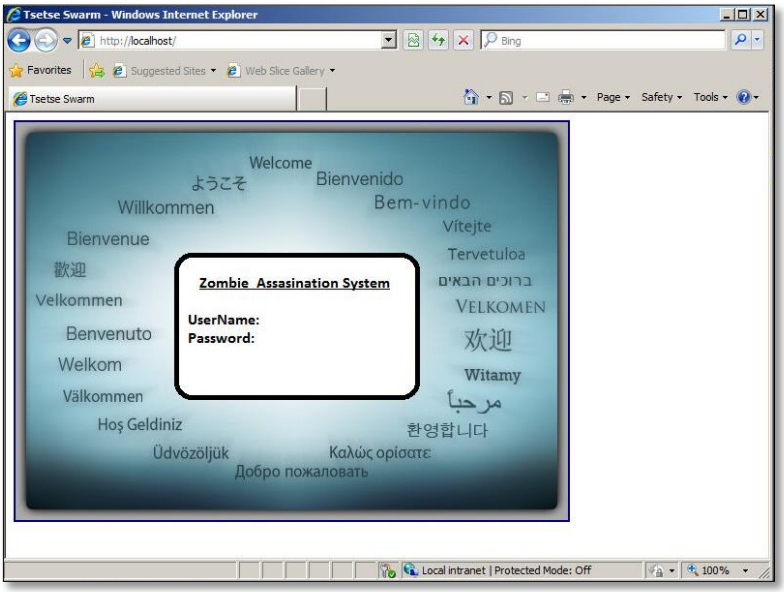
Automation

After deep analysis and many sleepless nights spent debating with myself (*the medication is starting to help though*) the need for Automation\Orchestration in this environment I have decided that if this scenario was real and given the limited resources and taking into account the technical requirements for a possible ZAS program (*I told you…many nights*) there is no justifiable need for any additional orchestration tool as the deployment\configuration automation provided by vCloud Director is more than able to orchestrate the deployment of customized virtual machines through the use of catalogs.

As example I have uploaded 2 vApp templates to the Tsetse organization catalog that can be configured and deployed via the organization web portal.



1. Tsetse_IIS_W2K8R2
    a. Deploys a Windows 2008 R2 VM with IIS installed
    b. Default website page has been customized to demonstrate the orchestration possibilities.
    (Have a feeling we've been here before)



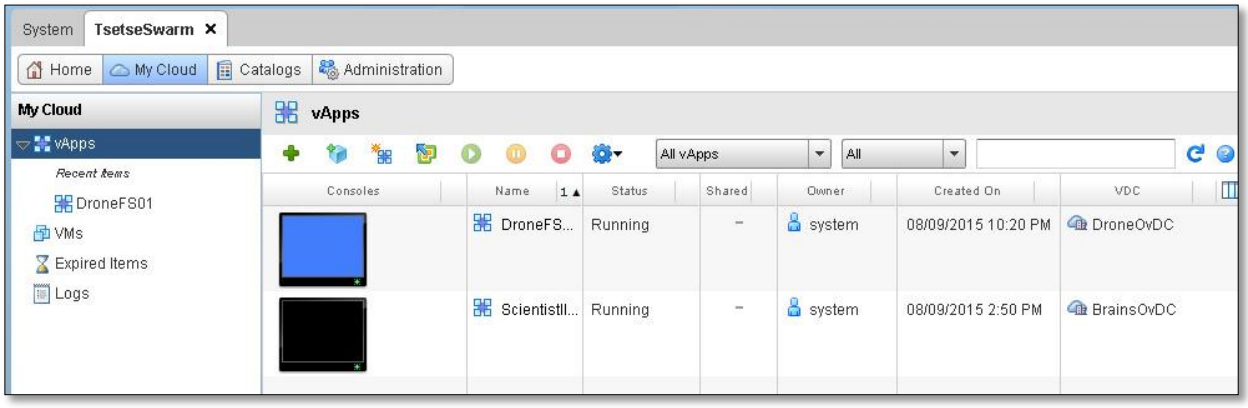
2. W2K8R2DC
    a. Deploys a standard Windows 2008 R2 image that can be used as a file server for the scientists' cat pictures.
    (Seriously am I the only one with this dejavu feeling?)

Deployment of the workloads is illustrated in Appendix A using the IIS server as example.

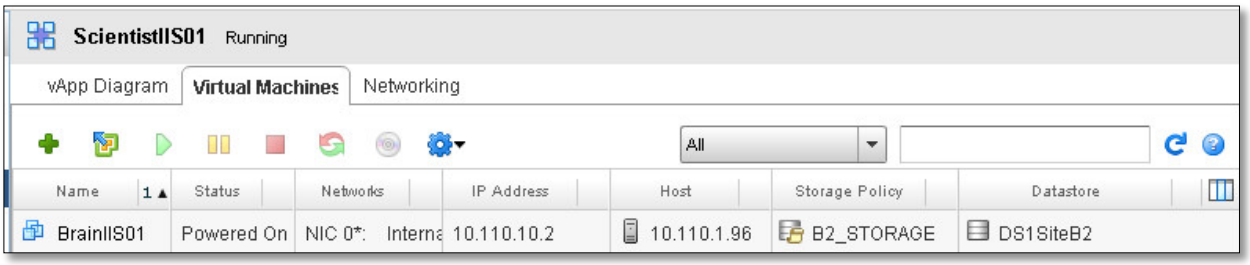
While I feel that this is enough to satisfy the requirements I have created Appendix B which illustrates how vCenter Orchestrator could be integrated and used to deploy a simple workload.

Organizational Workloads

2 workloads have been deployed as a proof of concept example.



1. A customized IIS frontend server (BrainsIIS01)



   a. Deployed from Org Catalog to BrainsOvDC
   b. Connected to the Internal Org Network
   c. Deployed to B2_Storage
   d. Running on Host VESXi02 (10.110.1.96) in the resource cluster

2. A fileshare server (DroneFS01)

   a. Deployed from Org Catalog to BrainsOvDC
   b. Connected to the Internal Org Network
   c. Deployed to A1_Storage
   d. Running on Host VESXi03 (10.110.1.130) in the resource cluster

Future planning

Physical resiliency

A short term high priority goal of the infrastructure team is to increase the resiliency of the physical layer and management VMs.

To accomplish this they will focus on 3 options:

- Setting up shared storage between the 2 physical sites so that a Metro cluster can be created across sites and vSphere HA options can be used.
- Adding additional hosts to each site with localized shared storage to create local HA clusters per site.
- Increasing the compute specs and storage capacity at each site to allow for cross site backups.

VCloud Director scaling

While the currently installed vCD appliance is pretty limited to scale it does serve the current and near future requirements. There is the possibility at a later stage that more resources could be found and a full installation on a Linux RHEL server could be deployed which would allow for up to 10 vCenters and 3000 ESXi hosts to be added per vCloud instance.

PVDC resource capacity

One of the near future objectives is to increase the resources available for the PVDC especially the compute and storage capacity in Site A. This can be done by adding an additional host to the Physical datacenter and adding its resources to the PVDC or (at least for the storage) adding an additional local disk to the Physical server and allocating this to the PVDC.

VCDX panel

The lead IT engineer has a new life goal to obtain his VCDX certification and get onto the VCDX judging panel before a certain female member of VDM judges (name withheld)…I'm thinking a design scenario using carrier pigeons to create a metro cluster.

References

Baremetalcloud. *Documentation*. n.d. <http://documentation.baremetalcloud.com/display/bmc/baremetalcloud+documentation>.

Coleman, Kendrick. *vCenter and vCloud Management Design - Management Separation*. n.d. <http://www.kendrickcoleman.com/index.php/Tech-Blog/vcenter-and-vcloud-management-design.html>.

Epping, Duncan. *Stretched vCloud Director Infrastructure*. n.d. <http://blogs.vmware.com/vcloud/2013/01/stretched-vcloud-director-infrastructure.html>.

—. *Thinking about a stretched vCloud Director deployment*. n.d. <http://www.yellow-bricks.com/2012/11/20/thinking-about-a-stretched-vcloud-director-deployment/>.

—. *VXLAN use cases*. n.d. <http://www.yellow-bricks.com/2012/11/02/vxlan-use-cases/>.

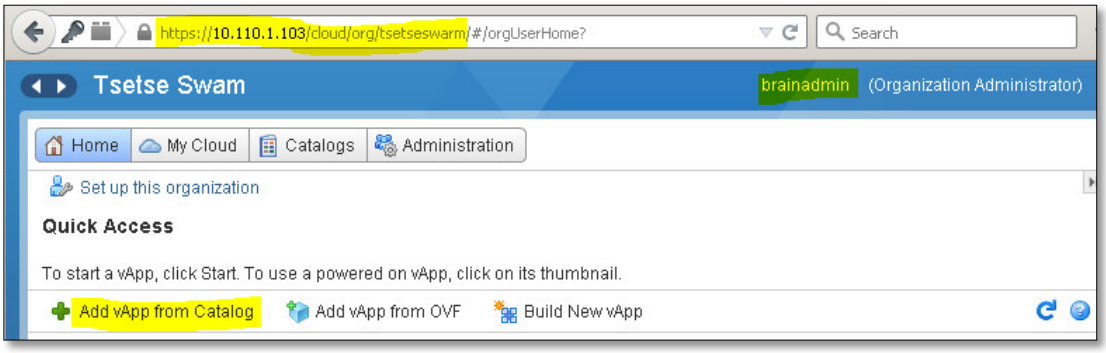
VMware. *vCAC 6.0 Documentation*. n.d. <http://pubs.vmware.com/vCAC-60/index.jsp#com.vmware.vcac.install.doc/GUID-800A0124-F721-45A5-B0D7-7420F106495E.html>.

—. *vCAT Documentation*. n.d. <http://download3.vmware.com/vcat/vcat31_documentation_center/index.html#page/vCloud%2520Architecture%2520Toolkit/000a.html#wwpID0EJHA>.

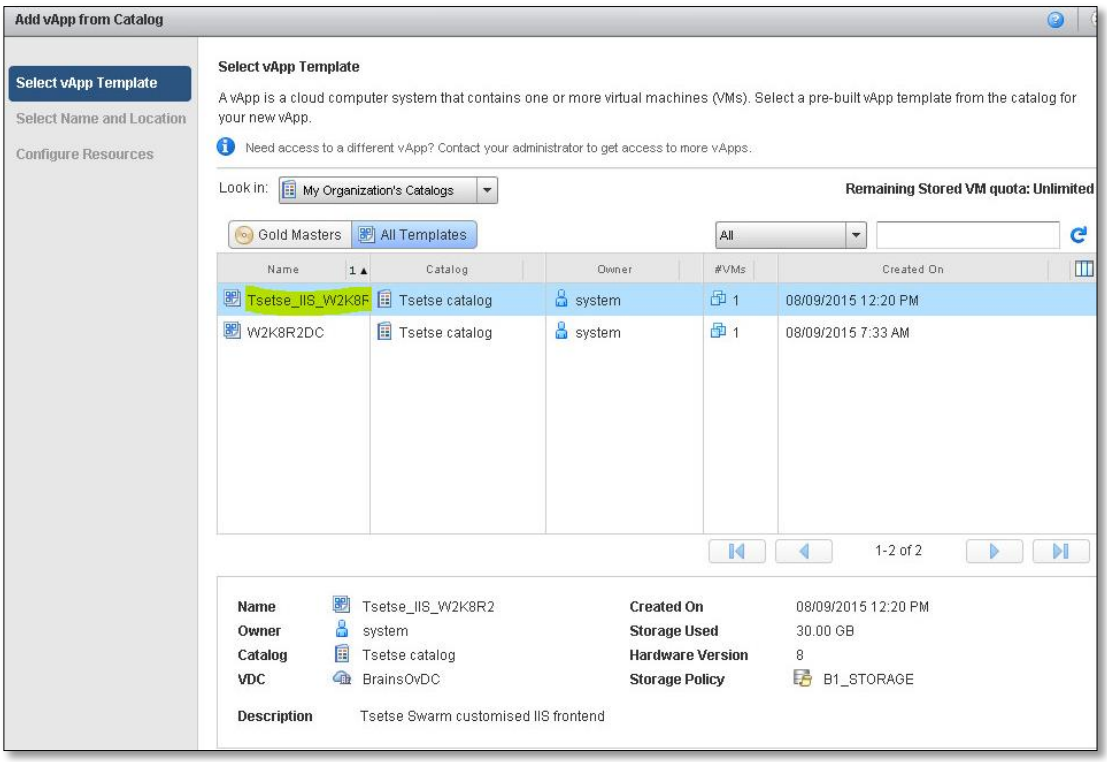
Appendix A – Workload deployment example

Deploying a workload with vCloud Director

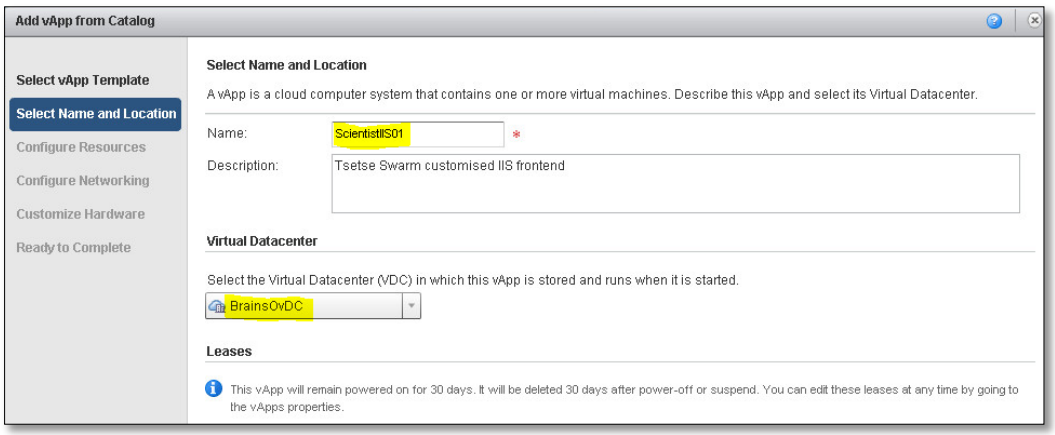
1. Log into the Organization specific URL: https://10.110.1.103/cloud/org/tsetseswarm using one of the local users (BrainAdmin in this case)



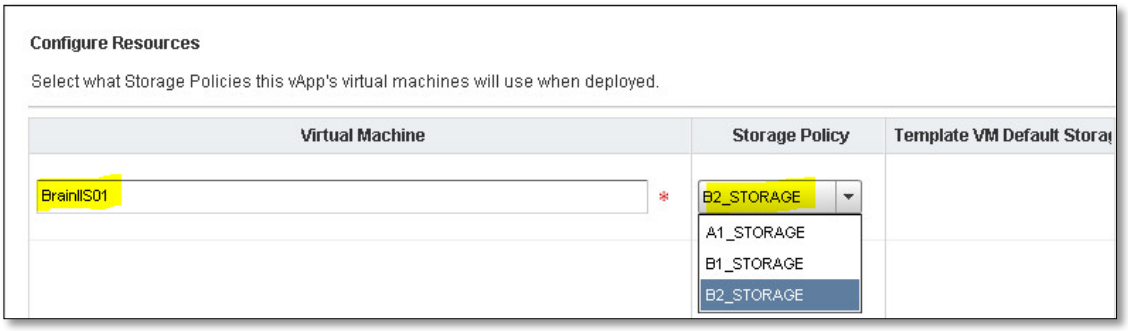
2. Select ' Add vApp from catalog'
3. Select the IIS template. (Template details are shown in the bottom field)



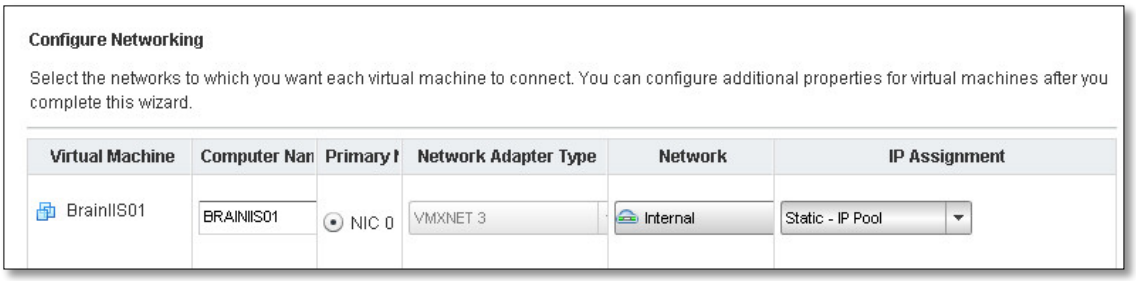
4. Give the vApp a name and check that it is going to the correct OvDC



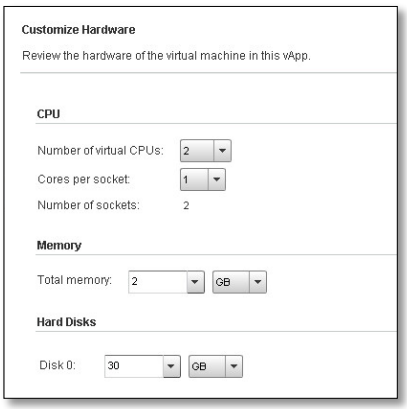
5. Give the VM a name and select the Storage to deploy it onto. In effect this is choosing a specific Site\Host.



6. Configure the NW to deploy it to and details

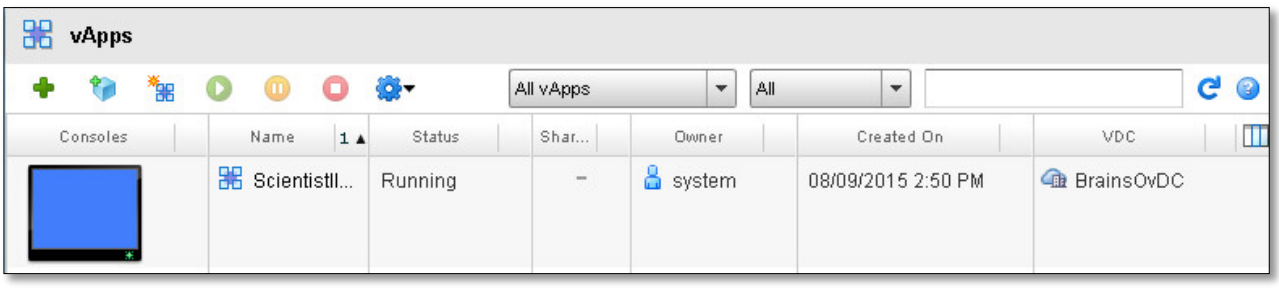


7. Customize the Hardware if needed.

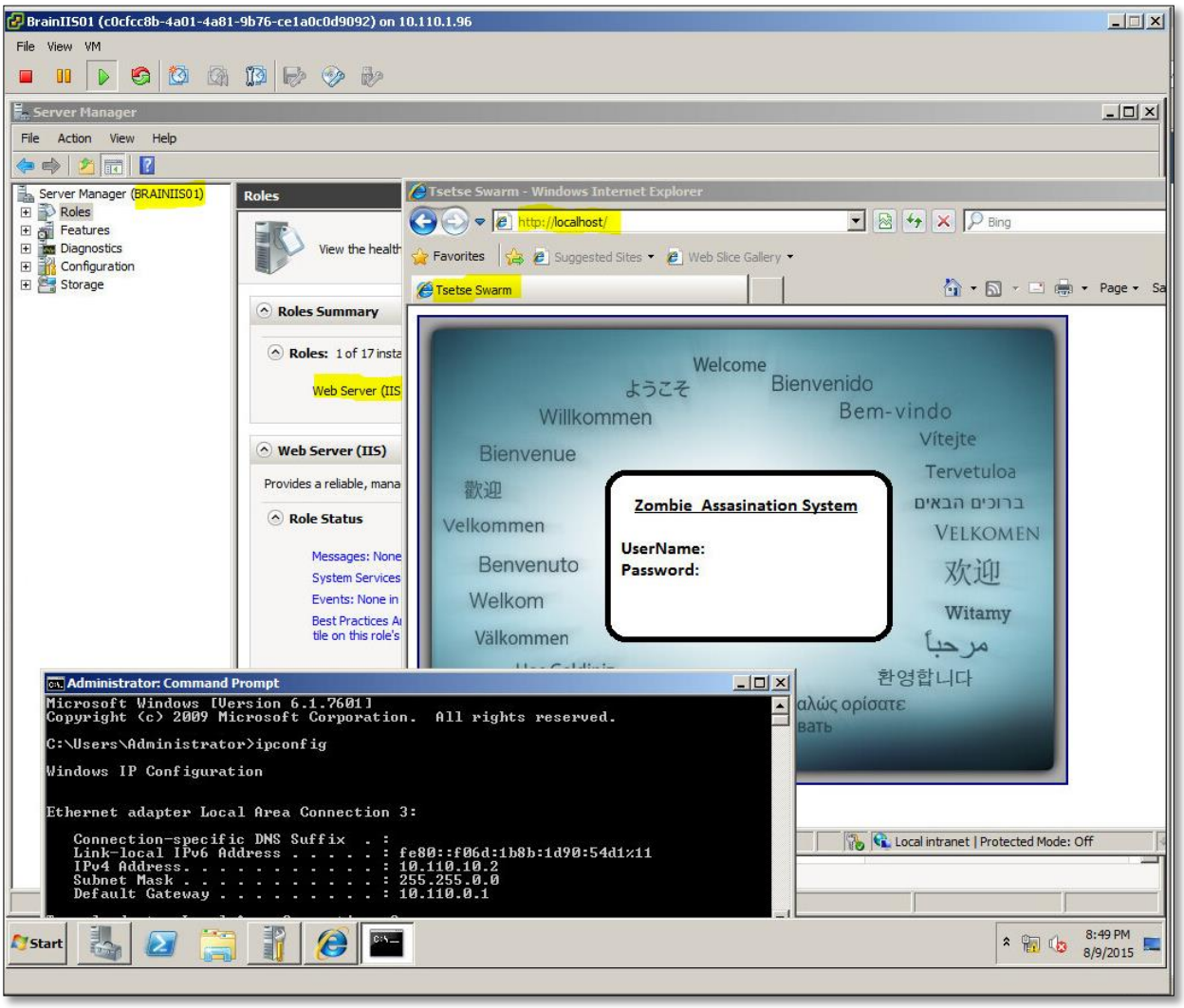


8. Click Finish and if all goes well you should see your vApp being created.
(Unless it is 00:53 on a Monday morning in which case it will most likely fail...)

9. And Voila. *(They really need to change the color of that screen, especially for Windows servers)*



10. And after the sysprep has finished running our newly deployed VM is configured and the customized webpage is available.



Appendix B – VCenter Orchestrator (vCO) integration

The following steps will walk through how to deploy the vCO appliance, integrate it into vCloud director and configure it to deploy an example workload.

VCO appliance deployment

The vCO appliance comes with an embedded Postgre database and requires 2vCPU, 3GB vRAM and 12GB disk storage.

1. The vCO appliance (.ova) is located (hopefully finished uploading by the time you read this) DC2LOCALDS1 datastore in the Images folder.
2. It is deployed as a normal .ova template
    a. Web client > Cluster > Deploy OVF template > Select vCO ova
    b. Give vCO appliance a name and choose where to deploy it.
    c. Select datastore and disk provisioning type (*hint: choose thin*)
    d. Select NW to join it to.
    e. Create a password and enter the IPv4 settings
    f. Select 'Power on after deployment' and click finish to begin the deployment.

Configure vCO for vCenter

1. Launch the vCenter Orchestrator Configuration web interface
    a. https://vCO_IP:8283
2. Login with username (VMware) and password you defined above.
3. Import your vCenter certificates
    a. Network > SSL Trust Manager > Import from URL > https://vcenter_IP:7444
4. Configure your SSO authentication
    a. Authentication > Select SSO Authentication
    b. Enter SSO URL : https://vcenter_IP:7444
    c. Enter SSO admin: administrator@vsphere.local and password
    d. Click ' Register Orchestrator'
    e. Click Update Orchestrator Configuration
5. Add your vCenter Server
    a. vCenter Server tab.> New vCenter Server Host
    b. Add vCenter Server
    c. Click Apply Changes
6. Configure Licensing
    a. Licenses tab > Select "Use vCenter Server license"
    b. Add your vCenter server details
7. Ensure that your plugins are enabled in the Plugins tab
8. Bind the vCO to a specific IP
    a. Network tab > In the IP Address box select the IP address that the vCO service should bind to
    b. Click Apply
9. Restart the vCO server service
    a. Startup Options
    b. Click "Restart service"

Configure vCO vCloud Director Plugin

1. Launch the vCenter Orchestrator Configuration web interface
2. Click on the "Install Application" tab
3. Browse for the vCloud Director Plug-in file and install it
4. After it is installed, select the vCloud Director Plug-in (on the left side of the Configuration screen)

5. Import your vCloud Director SSL certificates.
6. Click on the vCloud Director Plug-in in the left pane again
7. Now Click the tab: New vCloud Director Connection
    a. Fill out the form
    b. Select the shared session
    c. Specify 'SYSTEM' as the org name to configure the plugin for full administrative access over all Organizations and provide vCloud Director Server credentials.
8. Once plugin is installed, restart the vCO Server service.
9. Verify that the plugin is installed and configured correctly by clicking the Inventory in the bottom left of the screen.
    a. You should be able to browse through your vCloud Director Organizations.

Example workload deployment

As the deployment of workloads are simple enough using vCloud director this workflow will create a clone of a running vApp and deploy it in the OvDC.

1. Log in the vCO Client.
2. Click on the workflow tab > New Workflow
3. Give it a name (VDMclone)
4. Right Click on it > Edit.
5. Click the Schema tab.
6. Drag and drop a 'Workflow Element' onto the schema.
    a. Choose 'Clone vApp' for the workflow.
7. Right click the Workflow > 'Synchronize Presentation'.
    a. This will creates the input parameters and their presentation.
    b. Click save
8. On the schema > Select Clone vApp workflow > Visual binding tab
    a. Link the elements together

9. Go back to Schema and click validate.
10. Click ok to create the end element.
11. Save and close your workflow.

To run it right click it and click Start.

This will clone the vApp of your choice, configure it with a name of your choice and deploy it to the VDC.

Appendix C – Logins

Credentials

Component	IP	Account	Password	Role
Domain Controller	10.110.1.98	VDM\AwesomeAdmin	Spa1oo%s!	Domain Administrator
vCenter Server	10.110.1.74	VDM\AwesomeAdmin	Spa1oo%s!	Administrator
Vshield Manager	10.110.1.102	VDM\AwesomeAdmin	Spa1oo%s!	Enterprise Administrator
vCloud Director	10.110.1.103	VDM\AwesomeAdmin	Spa1oo%s!	System Administrator
Physical ESXi host 1	204.10.110.193	root	rQgjw5jJm9xP	root
Physical ESXi host 2	204.10.110.194	root	PM4bq468NDbD	root
VESXi01	10.110.1.96	root	Spa1oo%s!	root
VESXi02	10.110.1.127	root	Spa1oo%s!	root
VESXi03	10.110.1.130	root	Spa1oo%s!	root
TseTse OvDC	Org URL	DroneAdmin	Spa1oo%s!	Organization Administrator
TseTse OvDC	Org URL	BrainAdmin	Spa1oo%s!	Organization Administrator

Accessing the environment

Unfortunately with the Terminal server not up and running the simplest way would be to connect to the Physical ESXi host 1 (204.10.110.193) via vSphere client and open the vCenter server console. From there everything is available.