After the Outbreak

Project: Save the world!

Focus Area: VMware vSphere, Active Directory, SQL, Network, Storage, Remote Access

Prepared By: Jonathan Frappier @jfrappier www.virtxpert.com

Project Quality Plan Version Control

Version	Date	Author	Change Description
.5	8/4/13	Jonathan Frappier	Draft
1.0	8/8/13	Jonathan Frappier	Final

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

The world is in disarray after a virus outbreak that turned many into zombies. You've been recruited to build an infrastructure for a wealthy philanthropist to use in order to put the world back together.

1.1 Scope

Mr. Billionaire needs you to build him an infrastructure so he can continue his efforts across the globe. E-mail is key so teams can begin to communicate quickly, so is remote access to applications so the real planning can begin. His teams will also need a place to store and share their documents and data. He wants as many people as possible to have access to this infrastructure, and he wants it to be repeatable so it can be deployed in other places as more hardware is found.

There are 3 locations that must be use because there is not enough power in each of the locations to host all of the equipment. All three data centers are active sites. Assume that you have point-to-point network connectivity between your sites. Assume that you have to build for at least 5000 virtual servers in your primary site, 1000 virtual servers in your secondary site and 500 in your tertiary site. You must also have 3000 virtual desktops available for full desktop access and also mobile application delivery for at least 1500 devices.

A VMware vSphere (ESXi) 5.1 environment will be built to support the necessary applications and supporting infrastructure. VMware vCenter Server will be used to manage the virtual server environment. A second VMware vCenter Server will be used to manage the virtual desktop infrastructure. I have elected to use two separate vCenters due to the number of hosts involved in the design (ensuring per vCenter configuration maximums are not reached) and to separate management domains. The vCenter servers will be configured in Linked Mode; server infrastructure admins will be able to manage both the server and desktop infrastructure, the desktop infrastructure admins will only have access to the desktop infrastructure.

A Microsoft Windows 2008 R2 Active Directory based network will be built and configured to support VMware vSphere 5.1, VMware View 5.1, Microsoft Exchange 2010, Microsoft SQL Server, and Microsoft IIS. Windows 2008 R2 will be the default OS instance unless specific application requirements differ.

2 CURRENT STATE ANALYSIS

2.1 LAN & WAN

- **LAN**
  There is no current LAN infrastructure, all components need to be designed, configured and installed.

- **WAN**
  There is a 100Mbps connection at the primary site to the internet. There is a 100Mbps link between each of the 3 data centers. All public internet traffic for the secondary and tertiary sites is routed through the primary site.

2.2 Physical Servers

There is no current server infrastructure, all components need to be designed, configured and installed.

2.3 Storage

There is no current storage/SAN infrastructure, all components need to be designed, configured and installed.

2.4 SLA Definitions

No service levels were defined; will use 99.9% as a standard.

2.5 Site (Data Center) Locations

There are three (3) physical locations in which equipment is to be installed. Power and cooling is believed to support the necessary physical infrastructure to meet the following demands at each site.

2.5.1 Primary Site – BO01

The primary site currently has the power and cooling capabilities to support the entire physical infrastructure needed to support 5000 virtual servers and 3000 virtual desktops. There is a 100Mbps link to the secondary and tertiary site and a 100Mbps link to the public internet.

2.5.2 Secondary Site – BO02

The secondary site currently has the power and cooling capabilities to support the entire physical infrastructure needed to support 1000 virtual servers. There is a 100Mbps link to the primary and tertiary site.

2.5.3 Tertiary Site – BO03

The secondary site currently has the power and cooling capabilities to support the entire physical infrastructure needed to support 500 virtual servers. There is a 100Mbps link to the primary and secondary site.

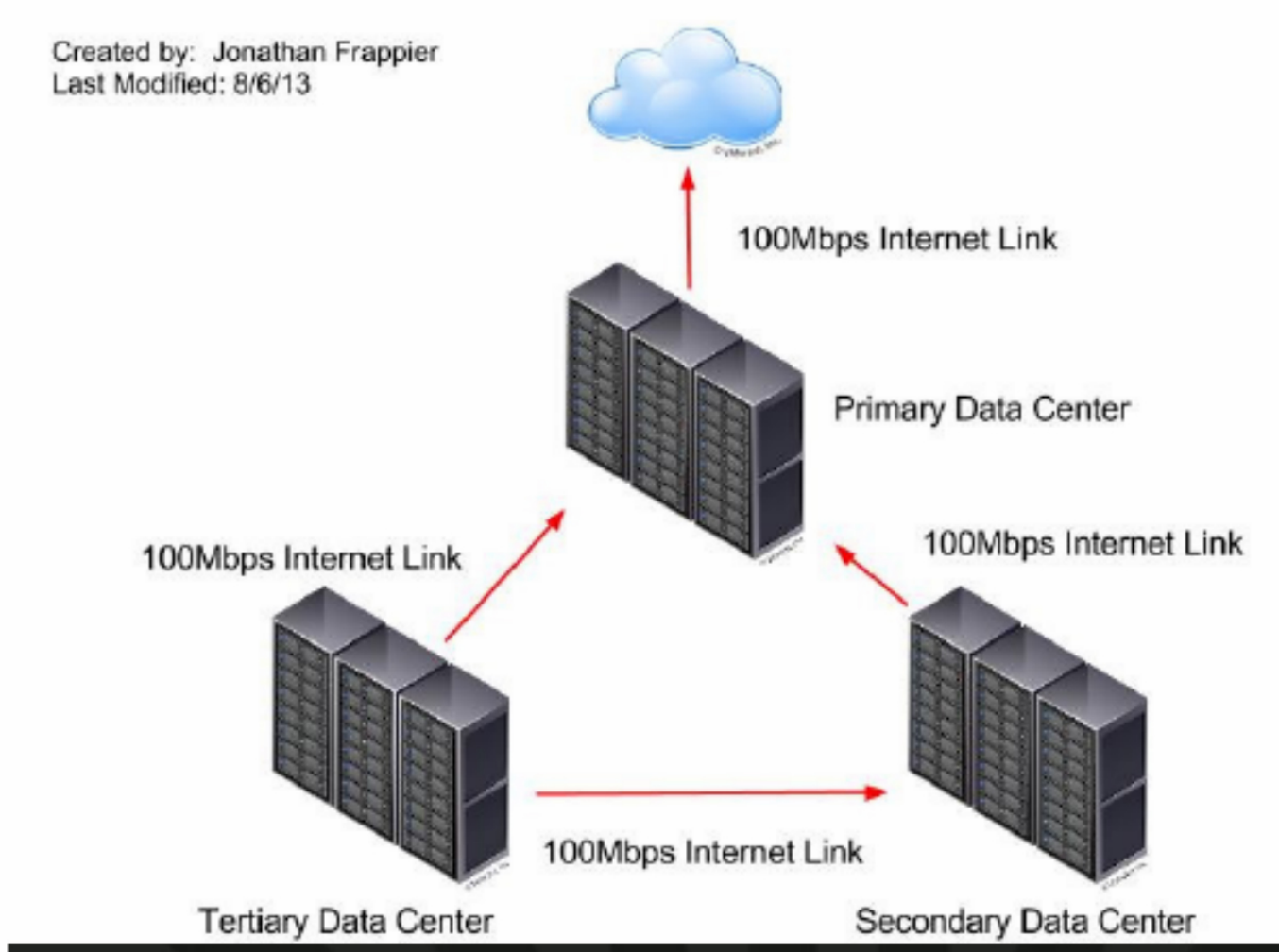
2.5.4 Naming Convention

Data centers will use the following naming convention:

LL##

Where LL is the location of nearest major city to the data center and ## is the numerical value for the order in which the data center came online. For example the first data center opened in Boston would be BO01. When a second data center is brought online in Somerville it would be BO02.

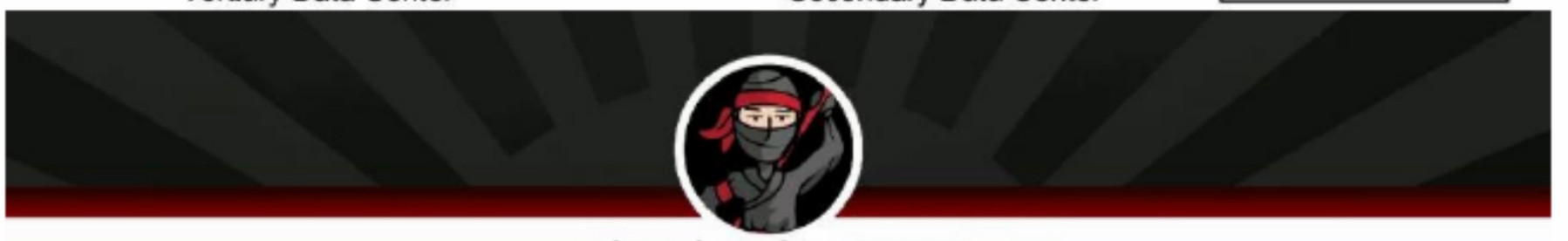
2.5.5 Diagram



The primary data center has a 100Mbps connection to the internet. The secondary and tertiary data centers route all public traffic through the primary data center.

Each red arrow is bi-directional.

In its current configuration, the primary data center is a single point of failure.



3 Requirements, Assumptions, Constraints & Risks

3.1 Requirements

The design must support public internet, email and application access to 3 physical locations. The required number of hosts will be determined per data center based on provided estimates in section 2.5.

3.2 Assumptions

- Since there are no previous workloads to monitor and define workload characteristics, both vendor and community published best practices will be used for a guide.
- Data centers are said to provide adequate power and cooling for the physical infrastructure necessary to support the VM capacity listed in Section 2.5.
- Racks, PDUs and necessary cabling are all available in the datacenter.
- Air conditioning and other environment stability is also assumed; cooling, raised floor designs or physical security aspects of the data centers is outside the scope of this design.
- Hardware available is believed to be reliable and in working order.
- A building block approach will be used for Microsoft Exchange server configuration guidelines supporting 2000 mailboxes per backend[1].
- A mailbox user profile of 150 messages sent per day will be assumed[1].
- One hundred (100) server VMs to a single physical host will be an assumed average consolidation ratio (100-to-1) for all data center locations.

- 50 physical hosts will be required to meet the assumed server consolidation ratio in the primary datacenter.
- 10 physical hosts will be required to meet the assumed server consolidation ratio in the secondary datacenter.
- 5 physical hosts will be required to meet the assumed server consolidation ratio in the tertiary datacenter.
- Three hundred (300) desktop VMs to a single physical host will be an assumed average consolidation ratio (300-to-1).
- 10 physical hosts will be required to meet the assumed desktop consolidation ratio.
- No growth estimates were provided; will assume minimal year over year growth and large expansion would result in additional data center locations due to power constraints in the current three data centers.
- The 100Mbps link will provide sufficient bandwidth for normal external traffic and internal management traffic such as AD replication, vCenter management of hosts and system monitoring.

3.3 Constraints

- Hardware is limited to stock on hand at a discovered warehouse; components are believed to be from 2008.
- Internet connectivity for all 3 physical locations will be routed through the primary data center; there is no direct internet access in the secondary or tertiary data centers.
- Because this is a new environment, there is no utilization metrics to base design decisions on. Assumptions will be listed where applicable.

3.4 Risks

- Internet connectivity for all 3 physical locations will be routed through the primary data center; there is no direct internet access in the secondary or tertiary data center making the primary data center a single point of failure for access to all three (3) data centers.
- Hardware available is believed to be reliable and in working order.
- The number of host required to meet the assumed consolidation ratio is above the maximum supported for a single cluster; multiple clusters will have to be used.
- No growth estimates were provided.
- Because this is a new environment, there are not utilization metrics available to create an adequate Admission Control Policy on.

4 Workload Definitions

4.1 Identified Applications & VM Sizing Estimates

Below are the following expected application groups and their expected resource requirements. Each system will have a corresponding template created for quick deployment of new systems.

- **Windows 2008 R2 Domain Controller (DC):** 1x vCPU, 4GB RAM, 30GB HD (C; OS) 60GB HD (D; Sysvol) 1 NIC
- **Windows 2008 R2 Exchange 2010 Client Access Server (CAS)[1]:** 2x vCPU, 8GB RAM, 30GB HD (C; OS), 60GB HD (D; Applications, Logs), 1 NIC
- **Windows 2008 R2 Exchange 2010 Transport Server[1]:** 1x vCPU, 8GB RAM, 30GB HD (C; OS), 60GB HD (D; Applications, Logs), 1 NIC
- **Windows 2008 R2 Exchange 2010 Mailbox Server (BE)[1]:** 4x vCPU 16GB RAM, 30GB HD (C; OS), 30GB HD (D; Application), 250GB HD (E, F, G; Exchange DB), 100GB HD (L; Exchange logs), 1 NIC
- **Windows 2008 R2 Standard Application Server:** 1x vCPU, 2GB RAM, 30GB HD (C; OS), 1 NIC

- **Windows 2008 R2 SQL 2008 R2 Database Server (for vCenter)[2]:** 4x vCPU, 16GB RAM, 30GB HD (C; OS), 100GB HD (D; SQL DB), 60GB HD (E; SQL logs), 60GB HD (F; SQL TempDB), 1 NIC.
- **Generic Server:** 1x vCPU, 4GB RAM, 30GB HD (C; OS), 1 NIC

4.2 Host Server Sizing and Information

HP DL580 G5 servers will be used (initial release date 2006[3]). Each server will be configured 4x Intel Xeon X7350 2.93GHz (initial release date Q3 2007[4]), 256GB RAM, 16x OCZ 32GB SSD SATA local drives. The SSD drives will be configured in a 2x drive RAID1 for the ESXi installation (32GB total space) and 14x drive RAID10 (7x drives strip, mirrored; 224GB total space) for host cache, VM swap file and additional emergency storage.

Each server is equipped with a two (2) port onboard 1Gbps Ethernet adapter. Additionally, two (2) quad-port (4 port) network interface cards (NIC) based on the Broadcom 5709 chipset will be added to each host for a total 10 ports. There is an Integrated Lights Out (iLO, out-of-band management interface) on each physical server for out of band management.

Each server will have four (4) single port 4Gbps Fiber Channel (FC) cards installed for connectivity to each of the datacenters two (2) storage array via a FC switch.

4.3 Storage Sizing and Information

EMC Celerra NS-480 storage arrays will be used in each location. The primary location will have two (2) physical NS-480's with 64TB total storage each to support the server and desktop infrastructure. The secondary data center will also have two (2) NS-480's; one with 64TB which will be replicated from the primary data center and one (1) with 32TB for local workloads. The tertiary site will have a two (2) NS-480's with 32TB of storage each; one for replication from the secondary site and one for local workloads.

4.4 Network Sizing and Information

Cisco Network equipment will be utilized for network connectivity. In the primary data center, two (2) Cisco ASA 5550 (estimated release date Nov 2007)[7] will be used for perimeter protection, public access control and VPN access. Two (2) Cisco 6513 series modular switch (estimated release date July 2007)[8] will be used for internal server connectivity in each data center. The 6513 can support up to eleven (11) line cards and a total of five hundred and twenty nine (529) 10/100/1000Mbps ports with two (2) supervisor management cards. While one switch should be sufficient to support the estimated fifty servers, each with ten (10) Ethernet ports, there would not be enough ports to include the HP iLO (out of band management interface) in that configuration and would also represent a single point of failure.

Each data center will run on a unique class B range (/16 or 255.255.0.0 subnet mask) sub-netted into VLANs for traffic segmentation. The Cisco 6513 operates at layer 3 and will handle routing between VLANs and access control lists between VLANs where appropriate.

Uplinks from each ESXi host will be configured as a trunk port to carry traffic for multiple VLANs. vSwitches will be configured with appropriate VLAN tags.

5 Active Directory Design

Microsoft Windows 2008 R2 Active Directory provides the foundation for VMware vSphere/vCenter installation and authentication. As such, a reliable Active Directory design must be considered. All Windows 2008 R2 Domain Controllers will be virtualized to leverage ease of backups, replication and VMware high availability features.

5.1 Domain Design

With high speed links between each of the three (3) data centers, a single Active Directory forest will be utilized. Each data center will run on a unique class B range (/16 or 255.255.0.0 subnet mask) with appropriate sites and replication settings configured to allow AD replication between each of the sites.

Four (4) domain controllers will exist the in the primary data center, two (2) each in the secondary and tertiary data centers.

The top level AD Forest will be named grimes.local and the primary AD site will be named rick.grimes.local. The subdomain is being used to allow future AD subdomains to be created if required even though we are utilizing only a single AD domain today.

Two (2) DC's in each data center will run DHCP to provide network information to hosts and other infrastructure via the use of reservations.

Each domain controller will be configured as an authoritative time source (NTP) and sync to pool.ntp.org. All servers and services within each data center will sync to their local DC's based on http://technet.microsoft.com/en-us/library/cc773263(v=ws.10).aspx

5.2 Naming Conventions

Domain: grimes.local
Primary AD sub-domain: rick.grimes.local
Future use AD sub-domains: lori.grimes.local, carl.grimes.local, etc…
Server names: Will use the following a naming convention:

LL##-TUUU##

LL## is derived from the data center in which the VM resides. T stands for type and will be used to identify **P**roduction, **T**esting and **D**evelopment systems. UUU will be a 2 or 3 letter designation to identify the type of system; examples include **APP** for generic application or file servers, **SQL** for database servers, **WEB** for web application servers (IIS, apache, etc). Other designations can be used as appropriate but should not include vendor specific names such as **IIS** in the event the Microsoft web server IIS is replaced.

Domain Controllers for each site will be named
Primary data center (BO01): BO01-PDC01 through BO01-PDC04, future use 05, 06, 07, etc…
Secondary data center (BO02): BO02-PDC01 & BO02-PDC02, future use 03, 04, 05, etc…
Tertiary data center (BO03): BO03-PDC01 & BO02-PDC02, future use 03, 04, 05, etc…

User accounts: There will be three primary types of user accounts:
Standard account: All users will be given a username of first initial followed by last name. In the event there are multiple users with the same derived username, a middle initial will be used. Further tie breakers will be determined on an as needed basis. An example username for Bob Smith would be bsmith@rick.grimes.local. For Lisa Smith it would be lsmith@rick.grimes.local.

Administrator accounts: These will be privliged accounts for individuals and will have the necessary rights to perform job specific functions above and beyond what standard accounts are able to perform. The format of these accounts will be: adm_usernamer. For example an administrator username for Bob Smith would be adm_bsmith@rick.grimes.local

The built in Administrator account will be renamed to Hershel Greene.

Service accounts: These accounts will be used to grant applications appropriate level system access in order to operate. Service accounts will follow the format of svc_servername where server name is derived from the actual server the application is to be installed on. For example a SQL server named BO03-PSQL01 would have a service account name of svc_bo03-psql01@rick.grimes.local.

6 Hosts

6.1 Physical Host Configuration

This section is for reference only, physical host configuration will follow the definitions in section **4.2 Host Sizing and Configuration**

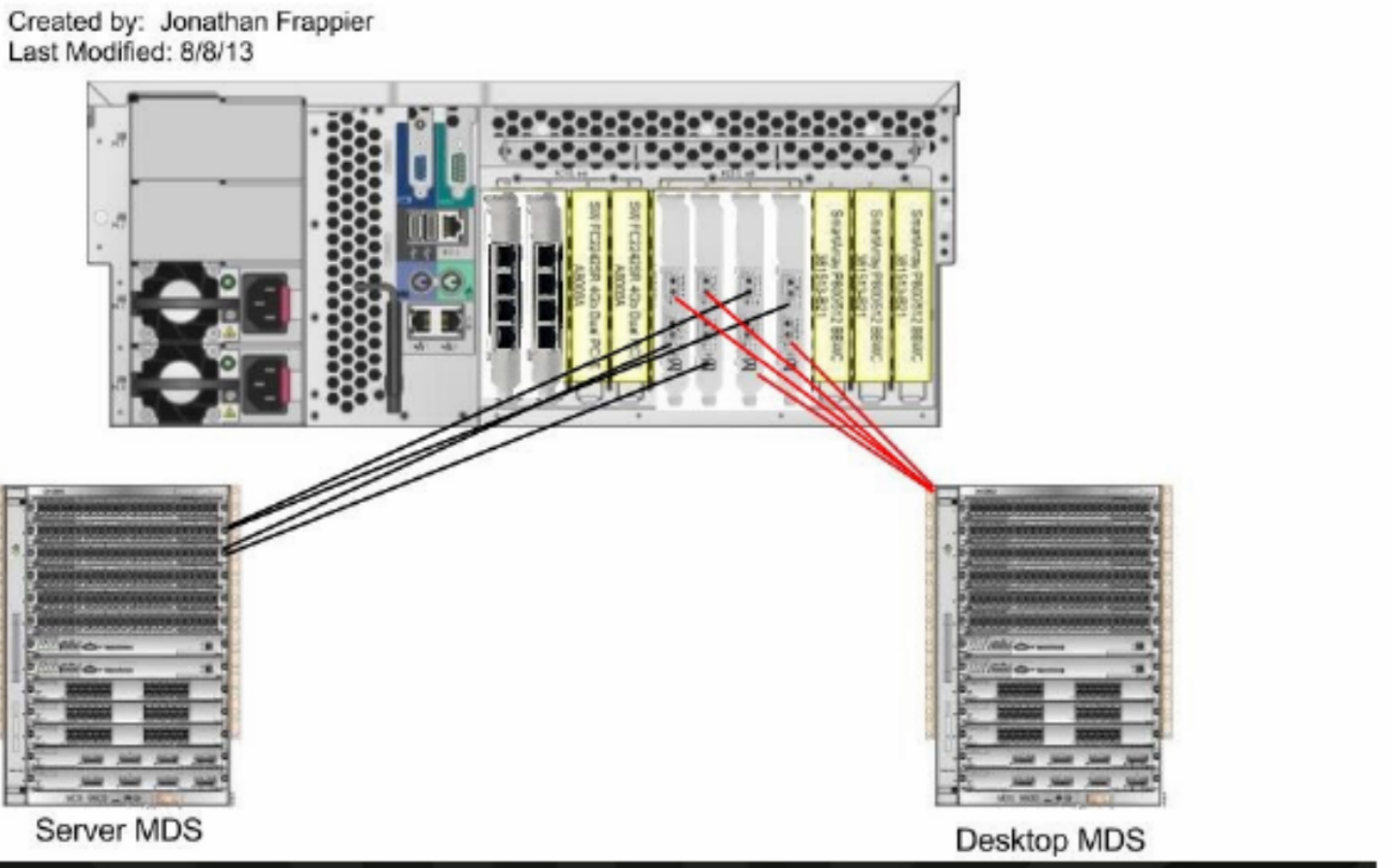
6.2 ESXi Host Configuration

Each host will be configured as noted below. Where applicable, the vSphere 5.1 Hardening Guide[8] will be followed.

Storage
A total of 40 shared LUNs (20 HP, 20 GP) will be presented to each host supporting the server VM infrastructure. Each LUN will contain a single VMFS data store.

A total of 20 shared LUNs (20 HP) will be presented to each host supporting the desktop VM infrastructure. Each LUN will contain a single VMFS data store.

Appropriate FC switch zoning, LUN to Storage Processor balancing, and other storage system configuration settings is assumed/will be documented in section 10.



Networking
Please see section 10 information on host networking configuration.

Power Management

Any server based power management features will be disabled or set to high performance to prevent processors from performing at lower speeds.

DPM will not initially be used.

Licensed Features
Each host will be licensed with VMware vSphere Enterprise Plus

Time Configuration
Each host will be configured to start NTP automatically and point to the domain controllers in their respective data centers.

DNS and Routing
DNS will be configured with to point to the domain controllers in their respective data centers. The default gateway will be the IP address of the VLAN on the network switch.

Authentication Services
Each host will be joined to rick.grimes.local to allow for user based authentication. The root password for each server will be unique, and secure and accessible only to the security department and CIO/CSO or CISO.

Virtual Machine Swap File Location
This setting will be configured at the cluster level and inherited by the host. Local SSDs are installed in each host and will be used for the VM swap file.

Host cache will be configured per server to swap to the locally installed SSDs.

6.3 ESXi Service Configuration

Service	Default	Start-Up Configuration
I/O Redirector	Stopped	Manual
Network Login Server	Running	Start/Stop with Host
Lbtb	Running	Start/Stop with Host
vSphere HA Agent	Running	Start/Stop with Host
Vpxa	Running	Start/Stop with Host
ESXi Shell	Stopped	Manual
Local Authentication (AD)	Running	Start/Stop with Host
NTP Daemon	Running	Start/Stop with Host
SSH	Stopped	Manual
Direct Console UI	Running	Start/Stop with Host
CIM Server	Running	Start/Stop with Host

6.4 ESXi Firewall Configuration

The ESXi Firewall Configuration will follow the vSphere 5.1 Hardening Guide[8], only the required ports necessary for day to day functionality will be enabled. Other services such as SSH will be enabled as needed for support purposes.

6.5 Local Authentication

Each ESXi host will be configured with a unique, secure root password. Host will be joined to AD to allow for per user based authentication. The root user should only be used when approved by the security group[9].

6.6 Lockdown Mode

When each host is joined to vCenter, Lockdown Mode will be enabled. This means the vSphere client cannot directly attach to a host for management. If direct management is required, a request can be

made to the security group to disable lockdown mode which can be done with local physical access or via HP iLO out of band management.

6.7 Host Profiles

Host profiles will be configured for each host to automatically create and configure vSwitch and VLAN information.

6.8 Host Monitoring

Host will be monitored by two applications, the first will be the built in vCenter Alarms[10] and by using Opsview which will also be leveraged to monitor individual VMs.

6.9 Naming Conventions

Physical hosts will follow a similar naming convention as outlined in section 6.2 - LL##-TESXRRUU

LL## is derived from the data center in which the VM resides. T stands for type and will be used to identify **P**roduction, **T**esting and **D**evelopment systems. For physical systems, RR will coincide to a physical rack location and UU to the top most U location in the rack. For example, the first host in the BO02 data center, in rack 1 with a top U location of 5 will be **BO02-PESX0105**, the next host in rack 1 with a top U location of 10 would be **BO02-PESX0110.**

---

7 vCenter and Cluster

VMware vCenter Server will be used to manage the virtual server environment. A second VMware vCenter Server will be used to manage the virtual desktop environment. I have elected to use two separate vCenters due to the number of hosts involved in the design (ensuring per vCenter configuration maximums are not reached) and to separate management domains. The vCenter servers will be configured in Linked Mode; server infrastructure admins will be able to manage both the server and desktop infrastructure, the desktop infrastructure admins will only have access to the desktop infrastructure.

A single vCenter server was selected to manage all three (3) physical data centers to simplify installation and management. A 100Mbps link between each of the data centers should provide adequate bandwidth for management and monitoring.

Each vCenter server will be protected by VMware vCenter Heartbeat as well as normal HA and backup defined practices.

7.1 vCenter

VMware vCenter server will be installed on a Windows 2008 R2 based VM. Due to the size of the environment a separate database server will be used. The vCenter server for both the server and desktop infrastructure will be identical.

7.2 vCenter Database

The vCenter server database will utilize Microsoft SQL 2008 R2 and will utilize the **Windows 2008 R2 SQL 2008 R2 Database Server** VM template (4x vCPU, 16GB RAM, 30GB HD (C; OS), 100GB HD (D; SQL DB), 60GB HD (E; SQL logs), 60GB HD (F; SQL TempDB)). All VMDK's will be think provisioned, eager zeroed to limit latency to do disk growth.

AD service accounts will be used and granted appropriate permission for SQL server to run.

The primary vCenter database will be configured in Full Recovery mode, all other databases will be in Simple Recovery mode. Local SQL backups will be configured to backup the vCenter database twice per

day, retaining 2 days local and transaction log backups every 2 hours. All other database backups will run twice per day retaining 2 days locally.

7.3 vCenter Services

Single Sign-On and the Inventory Service will both be installed on the same server as vCenter. SSO will be configured for multi-site to support Linked Mode between the server and desktop vCenter servers.

7.4 Cluster Configuration

7.4.1 Datacenter

A data center will be created for each physical location, for a total of 3 data centers within vCenter. The naming convention will following the actual data center name as defined in section 2.5

7.4.2 Cluster

The primary data center will be configured with multiple clusters, due to the limit of 32 host per cluster and an expected 50 physical host. The vCenter server managing the desktop infrastructure will not run into this limitation (expected 10 physical hosts).

The following BO1 clusters will be created

Mgmt: Initial inventory 4 physical hosts
Email: Initial inventory 8 physical hosts
Pub: Initial inventory 10 physical hosts
App: Initial inventory 28 physical hosts

7.4.3 HA

HA will be enabled for each cluster, Admission Control will be disabled initially until the environment has been running for 90 days. VM restart priority will be set to medium and isolation response to Leave Powered On. After 90 days an in-depth review of resource utilization will be performed to identify the appropriate Admission Control Policy and isolation response settings.

Datastore heartbeating selection will be left up to vCenter and not be manually overridden.

7.4.4 DRS

vSphere DRS will be enabled for each cluster. Anti-Affinity rules will be created to ensure specific systems do not reside on the same host in case of a host failure.

Included Anti-Affinity rules will include:

DC – Keep domain controllers on separate physical hosts
ExchCAS – Keep Exchange CAS servers on separate physical hosts
ExchMB – Keep Exhcnage Mailbox servers on separate physical hosts
vCenter (Primary DC only) – Keep the server and desktop vCenter server on separate physical hosts

Other application specific rules will be created when necessary.

Included Affinity rules will include:
vCenter-SQL – Keep vCenter and its SQL server on the same physical host. This should maximize communication between the VMs. One VM serves little purpose without the other in the event of a host failure so losing both at the same time is an acceptable risk.

Other application specific rules will be created when necessary.

7.4.5 vMotion

The vMotion configuration is listed in section 7 and is listed here due to the relationship with DRS.

7.5 vCenter Availability

To maintain vCenter availability, the following steps/resources will be utilized.

- Local SQL database backups for all related vCenter, SSO and inventory service databases and log files. SQL backups will be stored on a separate server and maintained for 30 days.
- VMware HA will restart the VM in the event of a host failure.
- vCenter Heartbeat will be used to create a replica vCenter server at the secondary data center.
- Unitrends Enterprise Backup will be used to create ongoing image backups which can be restored instantly if the VM becomes corrupt or otherwise unavailable.

7.6 vCenter Backup and Recovery

vCenter Backup and Recovery is out of scope for this design, since after all that is the next challenge.

---

8 Auxiliary vSphere Services

8.1 vMA

VMware vMA is an appliance to leverage command line access to vCenter and ESXi hosts. This will be installed and configured to support the environment.

8.2 vCenter Support Assistant

VMware vCenter Support Assistant is an appliance to automate the collection of log data to submit to VMware support. This will be installed and configured to support the environment.

8.3 vSphere Replication

Replication is outside the scope of this project.

8.4 vSphere Data Protection (or comparable Veeam etc..)

Backup and data recovery are outside the scope of this project.

8.5 Log Insight Manager (or comparable Syslog/Splunk etc…)

Log Insight Manager will be installed and configured to collect logs from all hosts and VMs.

8.6 Monitoring

Opsview will be used to monitor individual VMs, hosts and network equipment, however exact monitoring details are outside the scope of this project.

---

9 Storage

9.1 Storage Model Overview

The EMC Celerra NS-480 was chosen due to its multitude of available protocols, supporting Fiber Channel, iSCSI, NFS and CIFS. While the primary use will be over FC having the flexibility to deploy other protocols for specific use cases was considered ideal.

The NS-480 can support up to 480 drives, with 15 drives per Disk Array Enclosure (DAE) allowing LUNs to be created in increments of 7 or 14 drives with a hot spare available.

The three (3) units with 64TB total will use four hundred and fifty (450) 146GB 15K RPM Fiber Channel disks which will occupy thirty (30) of the thirty two (32) available drive shelves. The two (2) 32TB units will

use two hundred twenty five (225) 146GB 15K RPM Fiber Channel disks, utilizing fifteen (15) of the available shelves for a combined total of 256TB of shared storage.

One Celerra in the primary data center will be dedicated to the server VMs, the other to the desktop VMs. The Celerra for the desktop VMs will use only the high performance LUNs. The general purpose LUNs on the desktop Celerra will have select data from the server Celerra replicated to it for emergency purposes.

Local storage will be installed and configured on each server using sixteen (16) 32GB OCZ SSD drives. Two (2) drives will be used in a mirror for the OS install and scratch partition, fourteen (14) drives will be configured in a RAID10 for overflow and emergency storage giving each host 256GB usable storage space. We estimate a total of 60 ESXi hosts (50 for server, 10 for VDI) for a total of 19TB of local storage across all 75 ESXi hosts bringing the total amount of usable storage to 275TB.

A Cisco MDS9513 (estimated release date April 2006 based on release note reference[12]) will be installed in each data center, with two in the primary data center to support each production Celerra. The MDS 9513 supports up to 528 1/2/4/8 Gbps FC ports which will be sufficient the required number of servers.

The primary data center will leverage 4 Dual Port HBA's in each server, connecting to two MDS switches. The secondary and tertiary data center servers will leverage 4 Dual HBA's connecting to a single MDS switch.

9.2 Protocols

Fiber channel will be the primary protocol for host connectivity, however either NFS for CIFS shares can be created directly on the Celerra if required.

9.3 Storage Configuration

9.3.1 Interfaces

The NS-480 has two Storage Processors, to which 4 FC SFP's will be added (8 total, 4 in each SP).

9.3.2 Zoning Configuration

In the primary data center, server infrastructure hosts will be zoned to all LUNs presented from the Celerra through the MDS switch which supports the server infrastructure and only the replicated LUNs from the Celerra and MDS switch which supports the desktop infrastructure.

In the secondary and tertiary sites, all hosts will be zoned to all LUNs presented from the local Celerra through the MDS switch.

9.4 LUN Configuration

LUN's will be created based on the following configuration:

- **General Purpose**: 7x 146GB drives in a RAID5 with a hot spare (hot spare drives may be shared among up to 2 general purpose LUN's).
  - General Purpose LUNs will be used for non-critical or low volume application servers with an assumed usage scenario of 75% reads / 25% writes.
  - Example use cases may be web servers, file servers, domain controllers.
  - Raw capacity (not including hot spare): 1022GB
  - Usable capacity (after RAID utilization): 815GB[6]
  - Expected IOPS: 590 average random IOPS[5]
  - Expected number of General Purpose LUNs: 20 LUNs (150 total drives = 140 active drives + 10 hot spare) in each Celerra in the Primary Data Center.

- **High Performance**: 14x 146GB drives in a RAID10 with a hot spare (15 total drives)
  - High Performance LUNs will be used for performance-critical or high volume application servers with an assumed usage scenario of 50% reads / 50% writes.

- Example use cases may be database servers, email servers.
- Raw capacity (not including hot spare): 2044GB
- Usable capacity (after RAID utilization): 952GB[6]
- Expected IOPS: 915 average random IOPS[5]
- Expected number of High Performance LUNs: 20 LUNs (300 total drives = 280 active drives + 20 hot spare) in each Celerra in the Primary Data Center.

Secondary and tertiary sites will carry a similar ratio between General Purpose and High Performance LUNs.

Additionally 16x OCZ 32GB SSD SATA local drives. The SSD drives will be configured in a 2x drive RAID1 for the ESXi installation (32GB total space) and 14x drive RAID10 (7x drives strip, mirrored; 224GB total space) for host cache, VM swap file and additional emergency storage.

9.5 LUN Naming Convention

LUN's will be name in the following manner:

LL##-TLT##

Where LT = LUN type (GP or HP). For example the first High Performance LUN in the BO3 datacenter, where the Celerra is mounted in rack 3 would be (all LUNs are assumed to be production:

BO03-PHP01

The second HP LUN would be BO03-PHP02, and so on. VMFS datastores will be named to make the LUN it is created on.

9.5.1 Datastores

There will be a maximum of 1 VMFS datastore per LUN. Datastore names will match the names of used on the LUN. Please see LUN Naming Convention in section 9.5.

9.5.2 Storage vMotion

Storage vMotion is available as part of the VMware vSphere Enterprise Plus suite which is in use for this design.

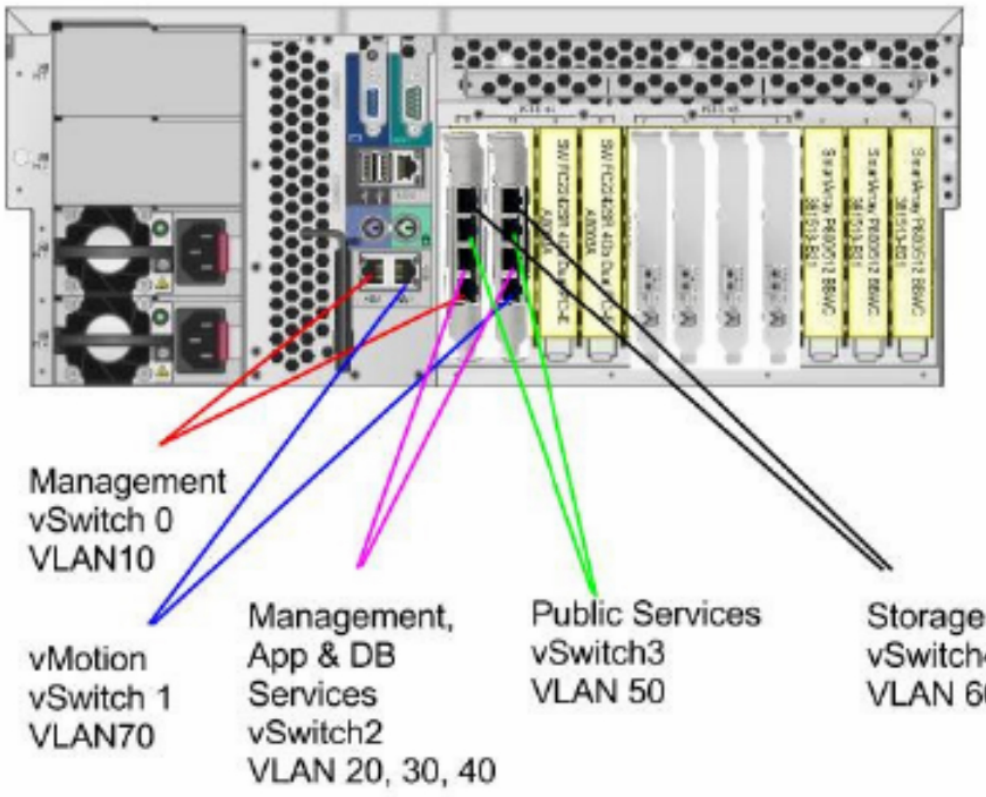
---

10 Network

10.1 Network Model Overview

Cisco Network equipment will be utilized for network connectivity. In the primary data center, two (2) Cisco ASA 5550 (estimated release date Nov 2007)[7] will be used for perimeter protection, public access control and VPN access. Two (2) Cisco 6513 series modular switch (estimated release date July 2007)[8] will be used for internal server connectivity in each data center. The 6513 can support up to eleven (11) line cards and a total of five hundred and twenty nine (529) 10/100/1000Mbps ports with two (2) supervisor management cards. While one switch should be sufficient to support the estimated fifty servers, each with ten (10) Ethernet ports, there would not be enough ports to include the HP iLO (out of band management interface) in that configuration and would also represent a single point of failure.

Created by: Jonathan Frappier
Last Modified: 8/7/13



NIC Port Pairings

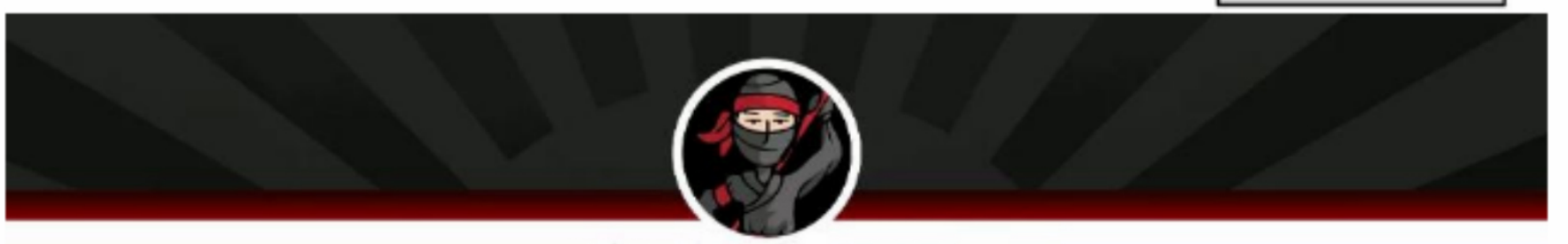
Onboard 0
PCI 1 Port 0

Onboard 1
PCI2 Port 0

PCI1 Port 1
PCI2 Port 1

PCI1 Port 2
PCI2 Port 2

PCI1 Port 3
PCI2 Port 3



10.2 Network Settings

Each data center will run on a unique class B range (/16 or 255.255.0.0 subnet mask) sub-netted into VLANs for traffic segmentation. The Cisco 6513 operates at layer 3 and will handle routing between VLANs and access control lists between VLANs where appropriate.

10.3 Port Configuration and Settings

Uplinks from each ESXi host will be configured as a trunk port to carry traffic for multiple VLANs. vSwitches will be configured with appropriate VLAN tags.

Physical interface ports will be hard set to 1000Mbps/1Gbps; full duplex is required/assumed as 1Gbps does not operate at half duplex. Servers will be manually configured as well.

VLANs will be created as follows along with a corresponding VLAN Interface:

VLAN1: Default VLAN; unused; shutdown
VLAN10: ESXi Hosts (Management interface)
VLAN20: Management VLAN (e.g. domain controllers, logging, monitoring, gateway to internet)
VLAN30: Database services (e.g. SQL servers)
VLAN40: Application services (e.g. applications accessible only from VPN or internet network)
VLAN50: Public internet services (e.g. public webservers)
VLAN60: Storage (e.g. backups, CIFS/NFS shares from Celerra)
VLAN70: vMotion traffic

10.4 Virtual Switch Configuration

There will be 5 Standard vSwitches configured on each host via host profiles. The vSwitches will be configured in accordance with the vSphere 5.1 Hardening Guide where applicable.

1. One (1) Standard vSwitch with 2 ports using onboard NIC port 0 as an active on vSwitch0 and PCI NIC1 port 0 as standby on vSwitch0 carrying traffic for VLAN10 (ESXi Management). The vSwitch will be configured to with 8 available ports (16 total per host).

2. One (1) Standard vSwitch with 2 ports using onboard NIC port 1 as an active on vSwitch1 and PCI NIC2 port 0 as standby on vSwitch1 carrying traffic for VLAN70 (vMotion). Multi-NIC vMotion will be configured.[11] The vSwitch will be configured to with 8 available ports (16 total per host).

3. One (1) Standard vSwitch with 2 ports using PCI NIC1 port 1 as an active on vSwitch1 and PCI NIC2 port 1 as standby on vSwitch2 carrying traffic for VLAN20, 30, 40 (VM/AD management, DB, internal applications). The vSwitch will be configured to with 248 available ports (256 total per host).

4. One (1) Standard vSwitch with 2 ports using PCI NIC1 port 2 as an active on vSwitch1 and PCI NIC2 port 2 as standby on vSwitch3 carrying traffic for VLAN 50 (public (e.g. web) applications). The vSwitch will be configured to with 248 available ports (256 total per host).

5. One (1) Standard vSwitch with 2 ports using PCI NIC1 port 3 as an active on vSwitch1 and PCI NIC2 port 3 as standby on vSwitch4 carrying traffic for VLAN60 (Storage, e.g. CIFS/NFS shares, backups). The vSwitch will be configured to with 248 available ports (256 total per host).

A total of 800 vSwitch ports will be configured per host; ESXi maximum per host is 4096 with 1050 active leaving 3296 available to be configured and 250 active assuming all 800 ports are active.

Physical network adapters will be configured at 1000Mbps/1Gbps Full.

10.5 Network IO Control

Network IO Control is only available on a Virtual Distributed Switch, where as we are using Standard Switches.

10.6 Network Configuration Backup

Indeni Dynamic Knowledge Base will be used to backup all device configurations and monitor for configuration changes.

---

11 Virtual Machines

11.1 Template Virtual Machine Settings

The following templates will be created based on VM function with the following specifications. These templates are only a guide and can be adjusted as needed to provide appropriate resources to each application.

- **Windows 2008 R2 Domain Controller (DC):** 1x vCPU, 4GB RAM, 30GB HD (C; OS) 60GB HD (D; Sysvol) 1 NIC
- **Windows 2008 R2 Exchange 2010 Client Access Server (CAS)[1]:** 2x vCPU, 8GB RAM, 30GB HD (C; OS), 60GB HD (D; Applications, Logs), 1 NIC
- **Windows 2008 R2 Exchange 2010 Transport Server[1]:** 1x vCPU, 8GB RAM, 30GB HD (C; OS), 60GB HD (D; Applications, Logs), 1 NIC

- **Windows 2008 R2 Exchange 2010 Mailbox Server (BE)[1]:** 4x vCPU 16GB RAM, 30GB HD (C; OS), 30GB HD (D; Application), 250GB HD (E, F, G; Exchange DB), 100GB HD (L; Exchange logs), 1 NIC
- **Windows 2008 R2 Standard Application Server:** 1x vCPU, 2GB RAM, 30GB HD (C; OS), 1 NIC
- **Windows 2008 R2 SQL 2008 R2 Database Server (for vCenter)[2]:** 4x vCPU, 16GB RAM, 30GB HD (C; OS), 100GB HD (D; SQL DB), 60GB HD (E; SQL logs), 60GB HD (F; SQL TempDB), 1 NIC.
- **Generic Server:** 1x vCPU, 4GB RAM, 30GB HD (C; OS), 1 NIC

11.2 Virtual Machine Authentication

All virtual machines will be joined to Active Directory and authentication to each VM will be validated by having a valid username and password.
The local administrator accounts will be renamed to Shane Walsh and the Guest account will be renamed to Daryl Dixon. The guest account will be disabled.

11.3 Virtual Machine Monitoring

VMs will be monitored by two applications, the first will be the built in vCenter Alarms[10] and by using Opsview which will also be leveraged to monitor VM hosts.

11.4 Virtual Machine Backup and Recovery

Unitrends Enterprise Backup will be used for VM backup and recovery, as well as backup of any CIFS or NFS shared created on the Celerra. Detailed configuration is beyond the scope of this project.

11.5 Naming Conventions

Server names will use the following a naming convention:

LL##-TUUU##

LL## is derived from the data center in which the VM resides. T stands for type and will be used to identify **P**roduction, **T**esting and **D**evelopment systems. UUU will be a 2 or 3 letter designation to identify the type of system; examples include **APP** for generic application or file servers, **SQL** for database servers, **WEB** for web application servers (IIS, apache, etc). Other designations can be used as appropriate but should not include vendor specific names such as **IIS** in the event the Microsoft web server IIS is replaced.

12 APPENDICES

12.1 Hardware Manifest

Device Type	Manufacturer	Model
Router	Cisco	7600
Firewall	Cisco	ASA 5540
Network Switch	Cisco	Catalyst 6500
Storage Switch	Cisco	MDS 9513
Server	HP	DL580 G5
Add-On NIC	Broadcom	5709 Based
Add-On HBA	EMC Qlogic	QLE2462-E-SP
Add-On HD	OCZ	32GB SSD

Storage Array	EMC	Celerra NS480
Storage Array	EMC	146GB FC 15K

12.2 Software Manifest

Vendor	Software
Microsoft	Windows 2008 R2
Microsoft	Windows 7 64-bit
Microsoft	Office 2010
Microsoft	SQL 2010
VMware	vSphere Enterprise Plus
VMware	Horizon View
VMware	Replication
VMware	vSphere Data Protection
VMware	Log Insight Manager
VMware	vMA
VMware	vSphere Support Assistant
VMware	vShield Endpoint
VMware	vCenter Server Heartbeat
Trend Micro	Deep Security
Opsview	Opsview Enterprise
Unitrends	Enterprise Backup
Indeni	Dynamic Knowledge Base

12.3 Reference

1 - http://goo.gl/7ohe4 - Microsoft Exchange 2010 on VMware Best Practices
2 - http://goo.gl/F2B4w - Installing vCenter Server 5.1 Best Practices
3 - http://goo.gl/ToZfWc - How old is my server
4 - http://goo.gl/PtlKT4 - Ark.intel.com
5 - http://goo.gl/LFBys - wmarow.com IOPS calculator
6 - http://goo.gl/xcF0h - RAIDcalc
7 - http://goo.gl/zRdhqT - Cisco 5500 Series Release Notes
8 - http://communities.vmware.com/docs/DOC-22981- vSphere 5.1 Hardening Guide
9 - http://goo.gl/WIC7Hb - vSphere 5.1 Documentation / Authentication
10 - http://goo.gl/KGJ7tK - vSphere 5.1 Host Conditions and Trigger States
11 - http://blogs.vmware.com/kb/2012/07/leveraging-multiple-nic-vmotion.html
12 - http://goo.gl/SEQfwH - MDS900 3.0(1) Release notes

12.4 VMware Configuration Maximums (double click to open PDF)

vmware

Topic

Configuration Maximums

VMware® vSphere 5.1

When you select and configure your virtual and physical equipment, you must stay at or below the maximums supported by vSphere 5.1. The limits presented in the following tables represent tested, recommended limits, and they are fully supported by VMware.

The limits presented in this document can be affected by other factors, such as hardware dependencies. For more information about supported hardware, see the appropriate ESXi hardware compatibility guide. Consult individual solution limits to ensure that you do not exceed supported configurations for your environment.

The *Configuration Maximums for vSphere 5.1* covers ESXi and vCenter Server.

Virtual Machine Maximums

Table 1 contains configuration maximums related to virtual machines.

Table 1. Virtual Machine Maximums

Item	Maximum
Compute	
Virtual CPUs per virtual machine (Virtual SMP)	64
Memory	
RAM per virtual machine	1TB
Virtual machine swap file size	1TB[1]
Storage Virtual Adapters and Devices	
Virtual SCSI adapters per virtual machine	4
Virtual SCSI targets per virtual SCSI adapter	15[2]
Virtual SCSI targets per virtual machine	60
Virtual Disks per virtual machine (PVSCSI)	60
Virtual disk size	2TB minus 512 bytes
IDE controllers per virtual machine	1[3]
IDE devices per virtual machine	4[4]
Floppy controllers per virtual machine	1
Floppy devices per virtual machine	2[5]
Networking Virtual Devices	
Virtual NICs per virtual machine	10[6]