CHALLENGE 1

Virtual Design Master – Season 2

Massey, Sean
seanm@seanmassey.net

Table of Contents

1 Executive Summary

Despite the efforts of Mr. Billionaire, the zombie outbreak has returned. The sudden appearance of a resurgent zombie horde has shattered resistance in many formerly secure areas. The position of the survivors on Earth has become untenable. Project Galactica, the contingency to evacuate survivors from Earth, has had its timetable pushed up, and a number of facilities need infrastructure to support the production facilities that will produce the evacuation spacecraft. The facilities, which are advanced manufacturing plants that resemble a cross between a modern automobile factory and a World War II-era bomber factory, will be expected to produce one launch-ready spacecraft every 72 hours once they are fully operational.

A pilot production facility near Cape Canaveral, Florida, has been pushed into full production using the test environment infrastructure.

Mr. Billionaire has tasked the IT Infrastructure Team with constructing the production environment infrastructure for Project Galactica. The compressed timetable of Project Galactica requires the existing infrastructure and supporting applications to be pushed into production globally without being fully developed, tested, and optimized. Because the workloads have not been finalized and will continue to receive frequent updates and new modules after it has been deployed, the infrastructure must be able to scale as the application stack grows.

The workloads that will be deployed consist of a web tier, an application tier, and a database tier. Message-queuing middleware is required so the various modules of the workflow can communicate.

The infrastructure that is being deployed must be orchestrated to reduce the manhours required for administration. It must be easily deployed as the engineering team will not be able to travel to the remote sites due to the safety risk from the zombie outbreak. High reliability is also a requirement as the infrastructure is supporting critical manufacturing processes.

2 Scope

The items that are in scope for this project are:

a. Design and implement the physical infrastructure for the spacecraft production facilities that are currently being constructed
b. Design a deployment strategy for the line of business applications and supporting infrastructure
c. Design and implement an automation strategy for the infrastructure
d. Design an availability solution for the production facilities to keep

The design outlined in this document will be implemented at all spacecraft production facilities as they come online.

3 Design Factors

The design factors section outlines the requirements, constraints, risks, and assumptions that the engineering team documented for the Project Galactica infrastructure.

3.1 Requirements

The Project Galactica spacecraft production facilities infrastructure has the following requirements:

1. Must scale to meet required demand
2. Must be highly available
3. Must be easy to deploy
4. Business Continuity/Disaster Recovery must be included in design
5. Must include an automation and orchestration framework to support physical and virtual deployments

The Project Galactica application stack has the following requirements:

1. Application Tiers
    a. Web Tier
    b. Database Tier
    c. Middleware Tier
2. Must be highly available

3.2 Constraints

Project Galactica has the following constraints:

1. Must be deployed in compressed timeframe
2. Must use the same hardware as the Cape Canaveral facility

3.3 Risks

The project team has identified the following risks:

1. Application development is not complete.
2. Developers insist on using custom software instead of off-the-shelf software.
3. Alternate spacecraft factories are still being built.
4. The Zombie Horde may impact hardware availability at some future date.
5. Operation of the global Internet could be disrupted

3.4 Assumptions

The project team has made the following assumptions:

1. Applications will perform poorly at initial deployment due to unfinished, untested, and unoptimized nature
2. The global Internet is still functioning
3. The Primary Datacenter used by Mr. Billionaire when rebuilding society following the first zombie horde outbreak is still operational and has available capacity.
4. The Active Directory and Microsoft Exchange environments implemented by Mr. Billionaire following the first zombie outbreak are still in use.
5. The skill level of the IT staff at the sites of the future spacecraft sites is fairly low
6. It is too dangerous for the members of the project team to travel to the remote sites

3.5 Best Practices

This is a new implementation with no operational baselines. Unless otherwise noted, vendor best practices will be followed.

4 Application Architecture

The applications used by the spacecraft production facility are built around a common set of technologies to facilitate easy development and deployment. The applications are three tier applications built using Microsoft's .Net Framework 4.5 and SQL Server 2012 with Service Pack 1. Business features are divided into independent modules, and the modules communicate with each other using message-queuing through RabbitMQ.

All applications are designed to be deployed on Windows Server 2012 R2.

The application modules that will be deployed in the first wave are:

1. Production Floor – Handles production floor activities and production scheduling
2. Inventory Module – manages materials and inventory control for production
3. Facilities Module – manages facility maintenance functions, records maintenance history, tracks preventative maintenance, and tracks equipment spare parts inventory
4. Launch Management Module – integrates with the launch managements systems, handles launch scheduling and passenger/crew manifests and notifications

The application tiers are:

1. Web Tier – The web tier presents the user interface. The interface is an ASP.net web form built with ASP.Net 4.5, and it interfaces with the business logic in the application tier.
2. Application Tier – The application tier contains the business logic for the modules. The application tiers are Windows Communication Foundation applications built using .Net 4.5. This tier interfaces with the web tier and the database tier. This tier also handles inter-module communications by passing messages through the RabbitMQ infrastructure
3. Database Tier – The database tier contains the datastore for each module. Databases are built built on SQL Server 2012 SP1 and interface with the application tier. Each module has its own database that is placed in an AlwaysOn Availability Group for high availability.

<insert diagram here>

4.1 Web Tier

The web tier consists of the servers that publish the module's web-based user interface. The web tier requires the IIS and Applications Server Roles with all role features installed and the .Net Framework 4.5 and Windows Process Application Service features with all sub-features installed.

Web Tier servers have the following hardware requirements:

- 2x vCPUs
- 4GB RAM
- 40GB Hard Disk (OS Volume)
- 60GB Hard Disk (Application volume)

4.2 Application Tier

The application tier consists of the servers that handle processing according to the programmed business rules. The processing layer is a Windows Communication Foundation Service built using .Net Framework 4.5. Communications between the application and web tiers are handled using HTTP.

Application tier servers require the IIS and Application Server services with all role features installed and the .Net Framework 4.5 and Windows Process Application Service features with all sub-features installed.

Application Tier servers have the following hardware requirements:

- 4x vCPUs
- 8GB RAM
- 40GB Hard Disk (OS volume)
- 60GB Hard Disk (Application Volume)

In order to guarantee performance of the application tier, a reservation of 100% of CPU and memory resources will be assigned. This reservation will be reviewed after 90 days to verify that it is still required.

4.3 Database Tier

The database tier consists of the servers that handle back-end database tasks. Each application module is provisioned with its own set of database servers. A minimum of two database servers are deployed with each module and deployed in an AlwaysOn Availability Group configuration. Database tier servers require the .Net Framework 3.5 and Failover Clustering features.

Database Tier Servers have the following requirements:

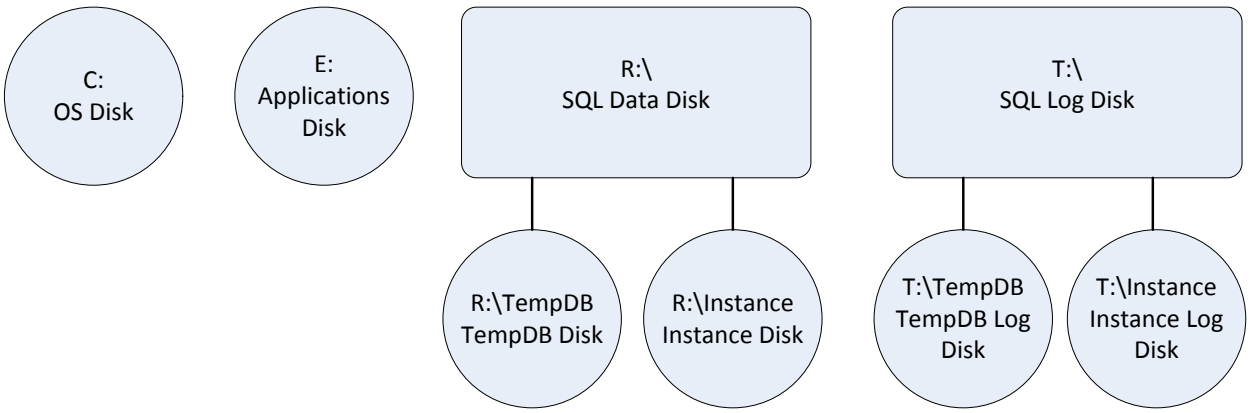
- 8 vCPUs
- 24GB RAM
- 40GB Hard Disk (OS Volume)
- 60GB Hard Disk (Application Volume)
- 200GB Hard Disk (SQL Backup Location)
- 2x Paravirtual SCSI Controllers for additional volumes
- 2x 3GB Hard Disks (Location for NTFS Mount Points to mount to)

Database servers are configured with Hot-Add CPU and RAM enabled to support dynamically increasing the resources assigned to the server.

Database servers require additional hard disks for storing the database files. These additional disks will be mounted as NTFS mount points to better distribute and control IO and formatted with a 64KB block size per Microsoft Best Practices. Volumes that store SQL Database files will mount under the R: drive and volumes that store SQL Logs will mount under the T: drive.

The following additional drives are required for a basic SQL Server deployment. These drives will be provisioned as Thick, Eager Zero virtual disks and connected to a paravirtual SCSI controller.

- 2x 20GB Hard Disk (TempDB and TempDB Logs)
- 2x 250GB Hard Disk (Application Instance data and log volumes)



In order to guarantee performance for the SQL Servers, a reservation of 100% of assigned CPU and RAM will be assigned.

4.4 Middleware Tier

The middleware tier handles communications between the different modules in the application. Inter-module communication is handled by a message-passing architecture built upon RabbitMQ. RabbitMQ was selected over other technologies such as Microsoft Service Bus or MSMQ due to RabbitMQ's improved support for high availability and message queue clustering.

Middleware Tier servers have the following hardware requirements:

- 2 vCPUs
- 8GB RAM
- 40GB Hard Disk (OS Volume)
- 60GB Hard Disk (Application Volume)

The specific Exchanges and Message Queues that will be deployed in the RabbitMQ cluster have not been finalized by the developers, and it is possible that these servers will need additional resources.

4.5 Active Directory

Active Directory is utilized by the applications for authentication, and Active Directory domain controllers are utilized for DNS resolution. Each spacecraft production facility will contain two Active Directory domain controllers that are a member of Mr. Billionaire's existing Active Directory environment.

The domain controllers will be placed into an anti-affinity DRS group to ensure that they are not placed on the same host.

The design of the Active Directory environment beyond ensuring that domain controllers exist in the site is beyond the scope of this project.

4.6 Authentication

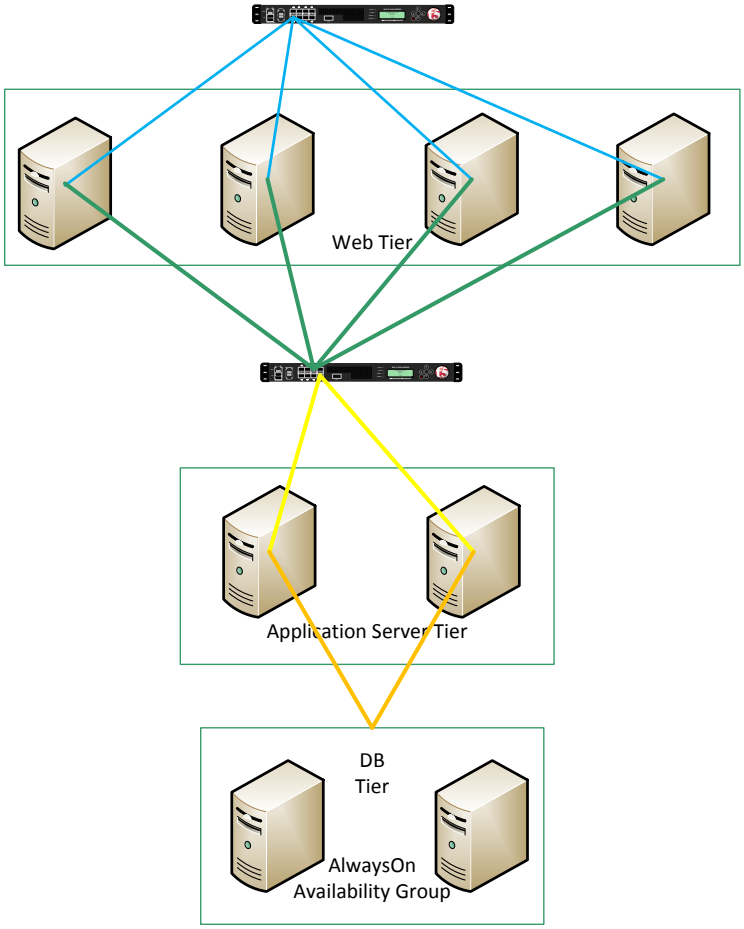
The applications are Active Directory integrated, and domain controllers will need to be available at each site to service login requests.

4.7 Service Accounts

Microsoft Managed Service Accounts will be used for running all services in the application stack in places supported by the vendors. Managed Service Accounts are special accounts that are restricted to the computers that they are assigned to run on, and the computer and Active Directory manage the password for the account automatically. IIS AppPools and SQL Server 2012 both support the use of Managed Service Accounts.

4.8 High Availability

The application infrastructure has been designed with high availability and horizontal scaling in mind to account for future growth.



High availability for the application is provided for all application tiers. The primary method of load balancing the web and application tiers is using clustered f5 Big-IP LTM virtual appliances. The web and application tiers of each application will receive a load balanced IP address and DNS name that clients will connect to, and the F5 appliances will route traffic to the least utilized servers. WMI health checks will be enabled to check the health of the load balanced servers in each load balancing pool, and rules will be configured to direct traffic based on the processor and memory utilization.

The HA feature provided by VMware will be utilized to restart virtual servers in the event of a host failure. The Fault Tolerance feature cannot be used because fault tolerance is not supported on virtual machines that have more than 1 processor.

High availability for the database tier is handled by the AlwaysOn Availability Group feature of SQL Server 2012.

4.9 Initial Deployment

The initial deployment for each module of the application will consist of the following servers:

- 4x Web Tier Servers
- 2x Application Tier Servers
- 2x Database Servers

4.10 Other Workloads

Other workloads may be required to support the operations of the spacecraft production facilities. These workloads include file servers, email servers, and other applications such as SharePoint, virtual desktops, or other custom software. Additional capacity is included in the cluster design to support these applications if they are required, but they are otherwise outside the scope of this implementation.

5 Systems Architecture

The systems architecture for the new facilities will be based upon the existing infrastructure at the Cape Canaveral facility.

5.1 Network

The network at the Cape Canaveral facility consists of four segments – a wide area connection, the local area network utilized for data services, an isolated industrial Ethernet network, and the data center network.

5.1.1 Wide Area Connection

The wide area network connections consist of a pair of 1GbE Metro Ethernet links sourced from two local providers. These connections provide direct point-to-point connectivity to the rest of Mr. Billionaire's network via the primary data center site.

Point-to-point Metro Ethernet was chosen for wide area network connection services because Metro Ethernet does not require BGP or other complex routing protocols like MPLS, provides a virtual private circuit between sites, and is easy to manage. Future spacecraft production facilities that are located outside of the United States, 1Gbps Internet circuits will be procured and site-to-site VPN connections with Mr. Billionaire's primary data center will be used to provide similar connectivity.

5.1.2 Local Area Network

The local area network provides access to data, voice, and application services. This network utilizes gigabit Ethernet Cisco switches to provide network data and voice services to users in the facility. An 802.11n wireless network is available for staff. Wireless network is provided by equipment sourced from Aerohive with an on-premises Hive Manager virtual appliance.

5.1.3 Industrial Ethernet

An isolated Industrial Ethernet network provides data services to the programmable logic controllers that operate the automated industrial machinery in the facility. This network is not accessible from the production data networks, and management of this network cannot occur from the production data networks. The industrial Ethernet is managed by the Production Engineering department and is out of scope for this project.

5.1.4 Data Center Network

The data center network provides both data networking and storage network services to devices within the local facility's data center. This network consists of two segments – a network for remote host management via Dell iDRAC cards installed in every server and a production network fabric for data and storage traffic. The hardware management network utilizes a single Cisco 3750X, and the production network fabric consists of a pair of Arista Networks 7050S-64 switches.

The production network fabric supports data and storage traffic between the Solidfire array and the

Arista 7050S-64 switches were chosen because:

1. The high port density for future expansion
2. The high throughput
3. Support for virtualization technologies built into the Arista network operating system
4. Can be managed from PowerShell when using PowerShell 5.0

<insert diagram here>

The network has six VLANs, five of which are on the Arista switches and one on the Cisco 3750X. The VLANs are:

VLAN	IP Range	Switch	Description
Management (VLAN 100)	10.x.100.0/24	Arista	Management VLAN for ESXi hosts
Data (VLAN 104)	10.x.104.0/22	Arista	Server Data VLAN for virtual servers
Private Cluster VLAN (192)	192.168.0.x/22	Arista	VLAN for private cluster network
iSCSI 1 (VLAN 251)	192.168.251.0/24	Arista	VLAN for iSCSI Port 1
iSCSI 2 (VLAN 252)	192.168.252.0/24	Arista	VLAN for iSCSI Port 2
vMotion (VLAN 250)	192.168.250.0/24	Arista	Network for vMotion
iDRAC Network	192.168.254.0/24	Cisco 3750X	Network for Host iDRAC

5.2 Physical Server Infrastructure

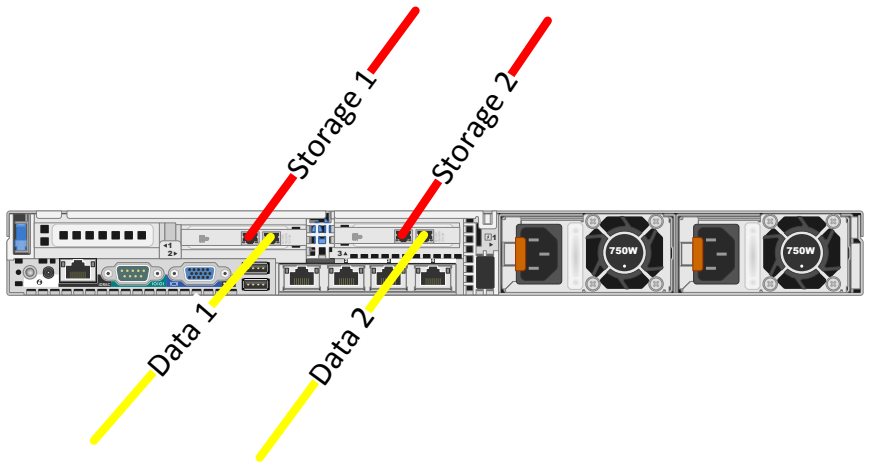
The physical server infrastructure for the spacecraft production facilities are based on Dell PowerEdge R620s running ESXi 5.5 Update 1. The specifications for these servers are:

- 2x Intel® Xeon® E5-2695 v2 2.40GHz
- 192GB RAM

- 2x Intel X520 DP 10Gb DA/SFP+ network cards
- 1x I350 DP 1Gb Ethernet, Network Daughter Card
- 2x 1100W Hot-Plug Power Supplies
- Internal Dual SD Module with 1GB SD Card with ESXi 5.5 Update 1 installed

The physical servers are equipped with a Dell PERC H310 RAID card, but they are not equipped with any hard drives or solid-state disks.

Dell hardware was chosen due to the IT staff's familiarity with the product lines. The servers were built with dual 10-core processors and 256GB of RAM to provide enough resources for resource-intensive virtual workloads. 10-core processors were selected to ensure that the deployed SQL Servers would fit within a NUMA node. Two dual-port 10GbE adapters were installed on the servers to provide redundant access to all VLANs and storage fabrics in the event of a switch or network adapter failure.



5.2.1 Server Quantity

In order to meet the needs of the projected application workload, vCenter, and Active Directory domain controllers, seven Dell R620 servers with the specifications listed in section 5.2 will need to be procured and installed in the environment.

5.3 Storage Infrastructure

The storage infrastructure for the spacecraft production facilities is based on the SolidFire storage platform. Solidfire provides a scale-out storage platform that can deliver both high performance and capacity, and it includes advanced quality of service features to ensure that the servers get the storage resources they need.

Connectivity to the Solidfire storage platform is provided by iSCSI over 10Gbe.

The specifications for the Solidfire storage environment are:

- Five-node storage cluster
- 60TB of usable storage
- 250K IOPS

Solidfire was initially selected as the storage platform for the development environment because it could provide the performance to support multiple development and test environments, build farms, and provisioning tasks.

It is being selected for the production environment for the following reasons:

- Provides enough capacity and performance to meet the unknown needs of the production application
- Uses 10GbE and iSCSI for connectivity. The IT staff has more experience with block storage protocols.
- IT staff was more comfortable with the more traditional nature of Solidfire compared to other scale-out and converged storage platforms.
- Solidfire provides a REST API that can be used with PowerShell for orchestration and automation

One point worth noting is that the exact storage needs for this application are not known because it is being deployed unfinished, untested, and unoptimized state due to the current circumstances. There is a good chance that many of the queries and stored procedures used by the application will perform poorly, and the initial plan to resolve this issue is to throw hardware at it until the developers can identify and resolve the issues.

Details on the logical storage configuration can be found in <link to section>

6 vSphere Architecture

VMware vSphere 5.5 Update 1 will be the virtualization platform used to run spacecraft production facility infrastructure. vSphere was selected over competing platforms because it provides best feature set for virtualizing Windows-based workloads and includes a management platform and orchestration engine.

The vSphere 5.5 Update 1 components that will be implemented in this infrastructure are:

- ESXi 5.5 Update 1 hypervisor with Enterprise Plus licensing
- vCenter Server 5.5 Update 1 Standard
- VMware Authentication Proxy

In addition to these components, the vCenter Orchestrator virtual appliance will be used as the Orchestration Engine for the environment. vCenter Orchestrator and the orchestration setup are described in

6.1 vCenter Configuration

vCenter Server is the management application for VMware vSphere environments. vCenter Server enables a number of features that will be utilized within this environment such as virtual Distributed Switch, HA Clusters, and Distributed Resource Scheduling (DRS).

vCenter includes a number of services that are deployed as part of the core vCenter Server install. These services are:

- Single Sign-On
- Web Client

- Inventory Service
- vCenter Server Core Application

The environment will contain a single vCenter server as a virtual machine running on Windows Server 2012 R2. All vCenter Server roles and the VMware Authentication Proxy will be installed on this VM. The vCenter databases will be SQL Server 2012 SP1 running on a separate server.

The vCenter Servers for all spacecraft production facilities will be installed in linked mode to allow administrators for remote management from a single vCenter Web Client.

6.1.1 vCenter Server Instance

vCenter Server will be a virtual machine running within this virtual environment. The specifications for the vCenter Server virtual machine are:

- 4 vCPU
- 24GB RAM
- 40GB Hard Drive (OS Disk)
- 60GB Hard Drive (Application Disk)

6.1.2 vCenter Database Server

The vCenter Server database will run on a SQL Server 2012 Standard SP1 instance. This database will be installed on a Server 2012 R2 server separate from the vCenter application. This server will have the following specs:

- 4vCPU
- 12GB RAM
- 40GB Hard Drive (OS Disk)
- 60GB Hard Drive (Application Disk)
- 200GB Hard Disk (SQL Backup Location)
- 2x Paravirtual SCSI Controllers for additional volumes
- 2x 3GB Hard Disks (Location for NTFS Mount Points to mount to)
- 2x 20GB Hard Disk (TempDB and TempDB Logs)
- 2x 250GB Hard Disk (Application Instance data and log volumes)

The TempDB and Application Instance disks will be formatted for a 64KB block size and configured as NTFS mount points.

6.2 vSphere Single Sign-On

Single Sign-On is a feature that was added with vSphere 5.1 to provide a central authentication source for vSphere environments. This feature is required for users to authenticate with vCenter and the vSphere Web Client.

Single Sign-On will be configured in multisite mode.

6.2.1 Active Directory Integration

The local Active Directory environment will be added as an authentication source within Single Sign-On. This will allow administrators in the environment to log into vCenter using their Active Directory user credentials.

The Active Directory domain will be configured as the default authentication provider within Single Sign-on so administrators. This allows administrators to log in without having to type the entire universal principal name for their username.

6.2.2 Single Sign-On Administrator

The Single Sign-On service includes a default administrator account called administrator@vsphere.local. This account has root level access to the entire vSphere environment. This account is the only account that can administer Single Sign-On when the environment is first configured.

This account will have a complex password.

For day-to-day administration of Single Sign-On, an Active Directory group will be created and added to the Single Sign-On Administrators through the vSphere Web Client.

6.3 vSphere Cluster Design

vSphere Clusters are a grouping of compute resources that are managed as one entity. Clusters enable VMs to be live migrated between hosts, and host that are in clusters usually have the same, or very similar, hardware and network configurations.

The environment will be configured with a single cluster. This will reduce management and setup overhead and enable resources to be utilized more effectively.

6.3.1 Cluster Sizing

The cluster will initially be configured with 10 hosts. This provides enough resources to run the initial workloads with one host reserved for HA failover. This also provides an additional 30% for growth in the event that new application modules come online or additional servers are needed to support the workload.

The number of hosts that were needed was based on the number of vCPUs that were assigned to virtual machines divided by the number of cores per host. The reason this method was used was because there is no existing performance data for the applications and because the application and SQL servers are receiving reservations equal to 100% of their assigned CPU resources.

The initial deployment of the spacecraft production facility application stack is predicted to have 8 database servers and 8 application servers for a total of 80 vCPUs. Since these servers are virtualized at a 1 vCPU to 1 core ratio, five servers would be required in order to meet the processor needs of these servers while having sufficient capacity to meet HA Admission Control policies.

6.3.2 vSphere High Availability

vSphere High Availability will be utilized to restart servers in the event of a host failure. This feature will be enabled on all production clusters.

HA Admission control is the feature that prevents servers from powering on if there are not enough host resources available to satisfy a failover event. This feature will be enabled, and failover capacity will be determined by a static number of hosts. Reserved failover capacity will be set at one host.

This option is preferred option in this environment since all hosts have the same configuration. If additional hosts are added, administrators will not need to figure out the new percentage of resources to reserve for HA.

6.3.3 vSphere Distributed Resource Scheduler

vSphere Distributed Resource Scheduler (DRS) is a feature that analyzes the current resource usage in the environment and balances computing capacity across hosts in a cluster. DRS will be enabled in the environment.

DRS will be fully automated to allow the system to manage itself without intervention from an administrator and set to a migration threshold of 4. This will enable DRS to execute most recommendation that provide a moderate improvement to the computing balance in a cluster.

In order to insure that two critical workloads are not placed on the same host for performance or fault tolerance reasons, DRS groups will be created. The groups that will be created are:

Group Type	Description	DRS Rule
SQL Server Anti-Affinity Rule	Rule to keep SQL Servers in an application group on different hosts	Separate Virtual Machines
Application Server Anti-Affinity Rule	Rule to keep application servers in an application group on different hosts	Separate Virtual Machines
Domain Controller Anti-Affinity Rule	Rule to keep Active Directory Domain Controllers on different hosts	Separate Virtual Machines
RabbitMQ Anti-Affinity Rule	Rule to keep RabbitMQ servers on different hosts	Separate Virtual Machines

Each application will have its own DRS rules for their SQL Servers and Application Servers. If additional servers are created for an application, they will be added to the correct DRS rule dynamically during provisioning.

6.3.4 vSphere Enhanced vMotion

vSphere Enhanced vMotion Compatibility is a feature that masks features on newer CPUs to ensure vMotion compatibility in clusters that have equipment with different processor generations. Enhanced vMotion Compatibility will be enabled and configured to use the “Intel Ivy Bridge” setting.

6.4 ESXi Host Configuration

All hosts in the vSphere environment will be running ESXi 5.5 Update 1 and primarily be managed by vCenter. The hosts will be configured as follows:

- Root Account will receive a complex password
- Hosts will not be joined to Active Directory, Authentication Proxy will be used for AD authentication
- Time Settings – NTP will be configured to start on host startup. NTP will be configured to receive time from us.pool.ntp.org.
- Syslog – A syslog server will be configured. The syslog server will be a LogInsight appliance cluster located at the DR site.

Lockdown will not be used on hosts.

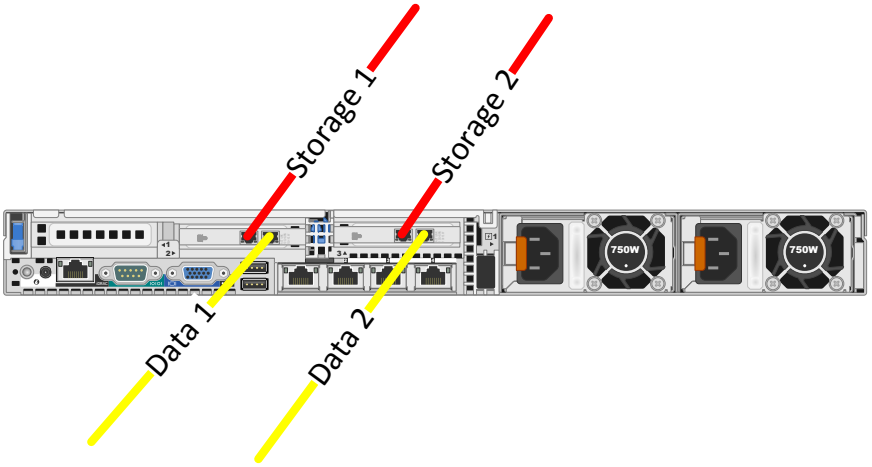
6.5 Virtual Network Design

There are three networks on each host. These networks are:

- A virtual distributed switch
  - Port Group for VM Data Traffic
  - Port Group for vMotion
  - Port Group for Cluster VLAN
  - Port Group for Host Management
- Standard Switch for ISCSI Port 1
  - ISCSI Port 1
  - Port Binding Enabled
- Standard Switch for ISCSI Port 2
  - ISCSI Port 2
  - Port Binding Enabled

Each host has two dual-port Intel 10GbE cards. One port on each card will be dedicated to storage traffic, and one port on each card will be dedicated to the Virtual Distributed Switch. The onboard 1GbE ports will not be used after the host Virtual Distributed Switch is configured.

The virtual distributed switch uplink ports will be configured as trunk ports for VLANs 100, 104, 192, and 250. The ports will be configured to use Load-Based Teaming to balance traffic across both uplinks.



6.6 Virtual Storage Design

The storage infrastructure for the vSphere environment will consist of multiple LUNs presented to the vSphere environment using the iSCSI protocol. The LUNs presented to the environment will be 750GB in size to keep the number of VMs stored on a LUN to less than 20.

Storage DRS will be enabled and placed in fully automated mode to manage storage resources. One large datastore cluster will be created with 12 LUNs. Storage IO Control will be enabled on these LUNs and integrated with the SolidFire quality of service features to ensure that the servers are receiving the storage resources that they require.

6.7 VM Template

One VM template will exist in the environment. This template will run Windows Server 2012 R2 and have the following hardware configuration:

- 2 vCPU
- 4GB RAM
- 40GB Hard Disk (OS Drive)
- 60GB Hard Disk (Application Drive)
- VMXNET3 Network Adapter

One customization specification will exist at each site to join the server to the domain and configure the IP address of the server.

Only one template is required because the orchestration engine will dynamically configure the server with the hardware, software, and Windows Server roles based on the role that it is assigned when it is deployed.

6.8 Monitoring

Monitoring of the vSphere environment will be performed by VMware LogInsight Manager and Quest Foglight for Virtualization Enterprise Edition. Configuration of these two products for the environment is beyond the scope of this document.

7 Orchestration and Automation

In order to manage an environment of this size with minimal staff, an orchestration and automation solution is required. The orchestration engine for the spacecraft production facilities will be vCenter Orchestrator, and PowerShell will be language that all automation components are coded in. The vCenter Orchestrator version that will be deployed is the 5.5 Update 1 virtual appliance.

vCenter Orchestrator was selected as the orchestration engine because it integrates with vCenter, provides a graphic workflow designer, and can manage Windows environments using a PowerShell plugin. The primary role of vCenter Orchestrator will mainly be to execute the various scripts called in the workflows. All of the tasks, including VM provisioning and application deployments, will be performed using PowerShell.

PowerShell was selected as the automation language because it will integrate with all components in the environment. Windows Server 2012 R2 was built with PowerShell management in mind, and, unlike previous versions of Windows Server, Windows remoting technologies are enabled by default. There are PowerShell commands for managing every feature in Windows, and many third parties have published their own sets of PowerShell commands or provide a REST API.

Because vCenter Orchestrator PowerShell module requires changes to the Windows remote management settings in order to run, Orchestrator will connect to a dedicated Windows Server to execute PowerShell scripts. To get around Kerberos authentication issues when connecting to remote servers from the scripting server, administrative credentials will be encrypted with a private cert and stored in an XML file. If the credentials are needed to execute a job, the script will decrypt the file and use the credentials at run time[i].

The modules that will need to be installed on the scripting server are:

- PowerCLI
- F5 PowerShell Module
- Veeam PowerShell Module
- Windows Remote Server Administration Tools

If a script requires additional information, such as location IP settings, the information will be stored in a SQL database and queried at run-time. This prevents complicated Select-Case statements and having to modify the script if changes occur.

Sample scripts are included with this design document. The sample scripts cover:

- Provisioning a VM
- Configuring a VM for SQL Server
- Installing SQL Server

The developers of the spacecraft production facilities software have indicated that they would like to deploy updates as frequently as possible. Workflows will be created using vCenter Orchestrator and PowerShell to allow publishing application updates to IIS across all application servers in the farm.

8 Disaster Recovery

In order to protect the environment against catastrophic failure and data loss, Veeam Backup and Replication will be implemented. Veeam will be configured to both back up servers and replicate them to a remote location.

Backup jobs will be saved to a local repository and then copied offsite using the Backup Copy job feature in Veeam 7. This will enable a grandfather-father-son backup rotation at the remote site.

The Replication feature will be used to make hot-spares of critical virtual machines in Mr. Billionaire's primary data center. In the event of a major systems failure, a failover to the remote site can occur and production can continue.

---

[i] See powertoe.wordpress.com/2011/06/05/storing-passwords-to-disk-in-powershell-with-machine-based-encryption/