THE FOUNDATION

Challenge 1 – Design and Orchestration

By Rob Nelson (@rnelson0)

THE FOUNDATION

Executive Summary

Establish a design for the manufacture and launch of Foundation colony ships and the supporting infrastructure. The infrastructure needs to be highly reliable and easy to deploy in future locations to maximize the number of launch facilities. The design emphasizes orchestration and automation to ensure manufacturing processes require minimal human input, increase overall efficiency and decrease defects in the material outputs.

This design supports the Foundation's manufacturing depot infrastructure, applications, and management. These include the manufacturing software, a 3-tiered application stack developed internally by the Foundation's developers; an automation and orchestration platform based on vCAC, Kickstart, Puppet, Gitolite, and Jenkins CI; and the Foundation's own *Encyclopedia Galactica*. The infrastructure and application platform is provided by a VMware-based private cloud. The design can to scale upwards, to support the predicted larger manufacturing needs of the next few years, and downwards, to face the anticipated resource constraints of the coming decades.

THE FOUNDATION

Detailed Background

The Foundation was established in 2008 in one of President Obama's earliest Presidential Orders, placing our benefactor, Mr. Seldon, at the head of the Foundation through 2018. Prior to the First Zed Outbreak (2013), the Foundation had a relatively minor budget, much smaller than even NASA's at the time. The charter was to develop the *Encyclopedia Galactica*, a combination of public databases, such as Wikipedia and the Human Genome Project, and any private databases the Foundation could acquire, that would encapsulate the combined knowledge base of the human race.

Through the first years, the Foundation's efforts to acquire private databases met with continual roadblocks. This frustration would ultimately be a positive development as it resulted in a diversification of the Foundation's interests. Using a combination of public grant money and Mr. Seldon's own personal wealth, the Foundation invested heavily in aerospace manufacturing, travel and tourism companies, such as Space X, along with numerous regional and national manufacturing firms and software development companies.

In the next 5 years, Mr. Seldon's Foundation grew from a small and ridiculed government agency with a single task to a large agency with no formal authority but a large reach into diverse interests throughout vital industries in America. As a result, the budget from the government continued to grow and fund further diversification… Until August, 2013.

At the time of the First Zed Outbreaks, the Foundation had already acquired Kennedy Space Center from NASA, having effectively assumed NASA's authority through Mr. Seldon's private holdings in the aerospace industries, and had established a small lunar base (Anacreon) months prior. While the United States government was attempting to suppress the first outbreaks, the Foundation was putting men on the moon again. When the unnatural "disease" was given the name Zed and a nation-wide emergency was declared, Mr. Seldon was able to privatize the Foundation, simultaneously making the Foundation the largest intact corporation on Earth and one of the few long term hopes for humanity.

Unfortunately, this came at a high cost. The first few weeks of the Zed outbreaks saw a rapid deterioration of society and industry. Some of the most brilliant minds of their generations were lost – including such notaries as Elon Musk, whose company Space X was subsequently granted to Mr. Seldon, and many prominent government officials including President Obama. Thanks to the rapid efforts of the newly inaugurated President Biden, plans were put in place to save as many of humanity's best and brightest as remained, many of whom are now either part of the Foundation or joining the wave of colonists.

THE FOUNDATION

Fred's dead

The abnormally severe winter of 2013/2014 slowed the Zeds and gave the world a chance to breath for a moment. President Biden formally declared the United States' priority to colonize the solar system and beyond to increase the chance for human kind to survive. Even more of the United States' stretched budget was allocated to the Foundation as a result, and a continual and sizeable military presence was provided to ensure the Foundation's security.

The Foundation's assets are located in Cape Canaveral, FL and the surrounding environs in facilities that are secure from Zed incursion. These include Cape Canaveral Air Force Station and the entirety of Kennedy Space Center - importantly Launch Complex 39 (LC-39), the Vehicle Assembly Building (VAB), the Headquarters Building, Launch Control Center (LCC), the Central Instrumentation Facility (CIF), and a revitalized Merritt Island Spaceflight Tracking and Data Network station (MILA). The city and facilities have come to be known as *Terminus City*.

Terminus City has been converted to the Foundation's headquarters and houses the ship building and depot facilities and launch pads. The shipyards are capable of producing an STS-sized colony ship within 72 hours while larger designs are in development. The initial destination for colony ships is the burgeoning Luna colony, Anacreon.

THE FOUNDATION

President Biden has provided the Foundation with three more launch sites and its construction divisions are in the process of building the manufacturing and launch facilities at each currently. An orbital construction facility, located at the Sun-Earth L2 Lagrange Point after the existing vehicles were relocated, has completed a colony module and launched it toward Mars, a focus of future colonization efforts. This summer's Second Zed Outbreaks threaten the development of these new facilities and the Foundation must be prepared to deploy rapidly to make use of the facilities before they are impacted or lost.

The VAB and nearby outbuildings house the majority of the manufacturing and computing systems that are in scope of this design. Other facilities, such as CIF and LCC, house electronics used for telemetry and launch control. These facilities are beyond the scope of the design as these purpose-built systems will not be virtualized. Remote access to the VAB network will be available in all facilities as necessary.

All facilities have continual US Armed Forces presence and they provide physical security, with few noted exceptions.

The Foundation is exceptionally well prepared for the task of colonizing the solar system and preserving the history of humanity. Its task to provide a virtualization and orchestration solution for a highly tuned manufacturing and launch process that will preserve the human race and its history, and it will succeed.

THE FOUNDATION

Overview

The virtualization solution primarily supports the 3-tiered manufacturing software. This application, developed by the Foundation, consists of the web front end (nginx), message queuing (RestMQ), and database (MongoDB), the VLAN networks, and software and hardware firewalls. These systems are housed within the VAB itself in specially constructed raised floor datacenter space with vastly excess HVAC capacity. The datacenter space also includes redundant power and network connections to every rack.

Additional components include the management platform, orchestration and automation engines, storage, networking, and security. The orchestration/automation system provisions and maintains the Infrastructure and Platform stacks and deploys the necessary Applications through continuous integration/development practices.

After manufacturing is complete, a replica manufacturing and datacenter system will be sent aboard each colony ship. There are no manufacturing facilities in space and these computer systems may be all the colonists have to rely on for years afterward, requiring a great deal of reliable and graceful degradation.

The system is designed to be able to scale both upwards as demand increases and down (to a minimum viable floor) as demand decreases, for instance during space transit or as hardware inventory levels drop over time.

THE FOUNDATION

Requirements

1. The solution should scale up and down to accommodate potential workloads.
2. Each manufacturing facility must be capable of working fully independently.
3. A minimum of three additional datacenters are planned.
4. Manufacturing systems must meet a 99.99% 24x7 service-level availability.
5. The infrastructure must be orchestrated to increase efficiency and eliminate errors.
6. The design must be highly reliable and easily deployable.
7. The design must provide the complete solution stack, from infrastructure to application.

Constraints

1. The Foundation has decided that a manufacturing system (or a replica) will be sent with every colony ship, including the computer systems. They must be serviceable by relatively skilled IT personnel not involved in the system's design or maintenance.
2. New systems/replicas must be assembled within the manufacturing timeframe (currently 72 hours) (see Requirement #6).
3. The design must incorporate the use of reliable, serviceable technology that can degrade gracefully over time.
4. The manufacturing application is an existing, internally developed 3-tiered application – client facing web layer, message queuing middle tier, database backend.
5. The Foundation has existing Active Directory services in the Terminus City campus.
6. The Foundation's mandate is to preserve humanity's history, in the form of the *Encyclopedia Galactica*, and attempt to capture impressions of the colonists and Earth to send with each ship.

Assumptions

1. The Foundation's budget and hardware cache ensures a steady supply of new hardware for the datacenter and ships.
2. The Foundation has acquired appropriate licensing for all vendor products (VMware, Microsoft, Red Hat, etc.) via government orders.
3. All specified hardware and software can be acquired and will work without Internet (on Earth) or wide-area network connections (in space).
4. vSphere administrators and developers have and can maintain the skillsets required to implement the solution.
5. Each colony ship will include one trained technician who can use, maintain, and repair the ship's virtualization platform.

Risks

1. There is no existing solution to measure anticipated resource requirements.
2. A lack of appropriate personnel (manufacturers, administrators, developers) may jeopardize the ability to maintain and improve the solution.
3. Zed activity may invalidate any or all requirements, constraints, or assumptions with no warning.

THE FOUNDATION

Hypervisor Design

ESXi v5.5 will be installed on rack mount servers via Auto Deploy stateful installation. The hosts will have 24 physical CPUs, 128 GB of RAM, a 32 GB SD card for hypervisor install, and access to shared storage. Management and VM traffic will be carried on redundant 1-Gigabit Ethernet interfaces. Storage and vMotion will be carried on redundant 10-Gigabit Ethernet interfaces. FCoE is the primary shared storage type; iSCSI is available future workload needs or domain failures require it. Each host will be joined to a cluster and managed from vCenter. Local access is for last resort in case of emergencies.

vSphere Management Layer

vCenter v5.5 with Enterprise Plus will provide centralized management of the ESXi hosts, VMs, and features. vCenter will be installed in a VM to ensure availability via vSphere HA and allow backups via VMware Data Protection Advanced, the chosen backup service (see VM Design). Because the upper scale is unknown and there is no migration path from VCSA to Windows, the Windows Server version will be used (see VM Design for OS specifics).

A Simple Install – all components on a single VM – provides scalability and maintains low complexity. If VM numbers exceed the ability of a Simple Install to manage, the components can be broken out by migrating the SSO and Database components to additional VMs. The Auto Deploy component will be installed on the same VM. Auto Deploy is used to deploy ESXi to new hosts.

vCenter SSO will connect to an Active Directory domain. Users will use the VMware vSphere Client or vSphere Web Client and their AD account information for all access to vCenter. See Security Architecture for more details

There will be no vSphere Update Manager (VUM). All patches will be provided via Auto Deploy and the use of an offline software depot; if contact is re-established with the west coast and updates are forthcoming this decision may be revisited.

vCloud Automation Center (vCAC) will be deployed to provide a self-service catalog where users can provision “X as a Service”, including additional instances of the manufacturing application, new Active Directory accounts, and change passwords. vCAC provides the front-end of the automation and orchestration engine required. See vCAC Portal and Puppet System for additional information on automation and orchestration.

THE FOUNDATION

Server Hardware

Cisco UCS C-Series rack mount systems have been chosen as the standard server hardware. The UCS platform is popular, well known, and there exists copious training material (such as #vBrownBag videos), making it an ideal choice for the dedicated vSphere admins and the colonists who will be trained to support it. Rack systems allow greater flexibility to scale up and down without the constraints and limited points of failure of a chassis-based system. If a single system fails, service levels gracefully degrade on the remaining systems.

Based on hypervisor design specifications, the UCS C460-M4 server has been chosen. This model has 2 1-Gigabit Ethernet interfaces for management and VM traffic and 2 10-Gigabit Ethernet interfaces for FCoE and vMotion. Each server has 4 E7-4809 v2 (6 core) CPUs for a total of 24 physical cores, a 32GB SD card for the hypervisor install, and 128 GB RAM. All storage will be shared. The system will begin with 6 servers. The number can increase or decrease, and if stockpiles of C460s run low, any other UCS C-Series hardware the Foundation acquires can be inserted with a minimum of changes to the overall system. The specific hardware manifest is found in the table below. The hardware will be connected to the network as described in the Networking Configuration section.

UCS C460 M4 base chassis w/o CPU/DIMM/HDD

Hardware Selections	Product ID#	Quantity
Power Cord, 200/240V 6A North America	CAB-N5K6A-NA	4
1400W AC Power Supply for 2U & 4U C Series Servers	UCSC-PSU2-1400W	4
32GB SD Card for UCS servers	UCS-SD-32G-S	1
Memory riser with 12 DIMM slots	UCSC-MRBD-12	8
Riser card with 5 PCIe slots	UCSC-PCIE-RSR-05	1
2 X 16 GB DDR3-1600 MHz RDIMM/PC3-12800 dual rank/x4/1.35v	UCS-MR-2X162RY-E	4
1.9 GHz E7-4809 v2/105W 6C/12M Cache/DDR3 1333MHz		4

THE FOUNDATION

Networking Configuration

Cisco Nexus switches work well with the Cisco UCS series and are offer a large number of Gigabit Ethernet ports, FCoE capability, and generous internal bandwidth. Like Cisco's UCS product line, the popularity of the Nexus switches ensures the systems are well known and training material exists for those unfamiliar with the product.

The VMware cloud's core will be a pair of Nexus 5672UP switches. The switches are capable for 72 10-Gigabit Ethernet interfaces with QSFP breakout cables, forty 1- and 10-Gigabit Ethernet interfaces, three fan modules and two power-supplies, providing redundancy within each unit. Each compute and storage device will be connected to both switches and the switches will cross-connect to ensure that complete or partial chassis failure of either switch does not constitute an outage. The switches will be configured according to Cisco's best practices guidelines to ensure efficient performance.

The models were chosen to provide room for growth or component failure. If workloads increase beyond 75% port utilization of any tier, the design will need to be revisited to properly accommodate growth without impairing long-term operational abilities.

The system will include a firewall (see Security Architecture) to connect to the greater Foundation network, for instance to interface with the inherited NASA/Space X telemetry systems or the administrative LAN. Colonist's systems will include a firewall as well, though no configuration will be performed as they will have no external network to connect to initially.

THE FOUNDATION

Shared Storage Configuration

Shared storage is required to allow VM workloads to migrate from ESXi host to ESXi host without impacting performance levels. Two types of shared storage have been chosen to meet different needs and provide long term operational continuity. NetApp provides business-class service levels and capacity. Synology provides lower service levels but better integrates with commercial systems such as video cameras.

NetApp is another commonly known vendor that personnel may already know or can learn quickly. Two E2624s will be configured to replicate to each other for data redundancy and availability. Each unit will be connected to two DE5600 shelves, fully stocked with 120 x 1.2TB SAS 10k drives for a total raw capacity of 144TB. Use of similar drives and shelves ensure redundancy within and across units and allows for easy component sharing as units degrade. The ESXi hosts will use these as primary shared storage.

Four 8GB FC and four 10GB iSCSI interfaces provide ample bandwidth and high redundancy/availability between the NetApp and the network. Shared storage will use Fibre Channel. The iSCSI interfaces will be used to synchronize Synology data.

Synology is also a commonly known vendor and uses a DSM OS with a web based interface that is easy to learn and use. A RS2414+ with 4GB system RAM and 12 x WD Red 3 TB SATA III provides 36 TB raw storage. The Synology system will be used to record surveillance system video in and around the computer facilities (particularly of construction itself), video journals of all personnel involved in spaceship construction and computer systems operation, and will also include a copy of *Encylopedia Galactica* (rumors that Mr. Seldon has included secret instructions are decidedly *not true*). The surveillance records and video journals are designed to provide context to the colonists who need to maintain their equipment at the destination. The ESXi hosts will not be configured to use the Synology's storage.

Four gigabit Ethernet interfaces will be bonded together to provide a highly available logical connection to the network capable of supporting the modest bandwidth requirements of the security system. The bonded interface will carry two VLANs. The first VLAN is shared between the Synology and NetApp and uses iSCSI for replication. The second VLAN is shared between end users and the Synology and uses iSCSI and NFS. This separation ensures end users do not have direct access to the NetApp storage, protecting the shared storage from end user access, and allows the Synology and NetApp to communicate. Synology DSM also supports both iSCSI and NFS, offering a workaround for systems that encounter NetApp degradation or failure.

THE FOUNDATION

VM Design

Initial system VMs are described here. See the vCAC Portal section for additional VMs that may be provisioned by end users.

As described, Microsoft and Red Hat Enterprise licenses have been acquired. Windows Server 2012R2 Datacenter Edition and Red Hat Enterprise Linux (RHEL) 7 are the most recent server editions from each vendor. Windows licensing allows the installation of 2012R2 or any previous Windows Server edition. All workloads are supported on these two platforms, which will be used throughout the design.

As there is no previous design to compare to, all resource allocations are estimations based on a combination of vendor guidelines and community best practices. Resource usage will be recorded via vCenter and requirements will be revisited after 30 days.

The VMs in the vSphere cloud can be broken into two general groups. Management includes the vSphere-centric VMs as well as the automation and orchestration engine. Manufacturing encompasses the manufacturing application and its attendant services. Some services may involve both systems; these will be classified as Management.

Management services

There is one installed set of management VMs. Clustering or distributed service guidelines will be followed according to vendor best practices if the workload determines that service levels are insufficient.

Windows Domain and vCenter

General LAN and End User access requires integration with the existing Active Directory forest. A new domain tree will be created and two Windows 2012R2 VMs will be provisioned as domain controllers for this tree. Windows 2012R2 Datacenter licenses have been acquired and all additional Windows VMs will also run 2012R2 unless otherwise specified. Additional domain-related VMs include RDP servers for remote access and management stations, an RDP Licensing Server. The vCenter server will be installed on Windows as well. This table lists the initial resource allocations and VM quantities.

Service	vCPUs	RAM (GB)	System disk (GB)	Data disk (GB)	Quantity
Domain Controller	2	8	60	0	2
RDP Session Host	2	32	60	300	4
RDP Licensing	1	4	60	0	2
vCenter	4	32	100	1000	1

vSphere Systems and Appliances

vCAC is an important part of the automation and orchestration of the private cloud. vCAC v6.0 requires four additional VMs: the Identity Appliance and vCloud Automation Center Appliances are deployed from OVF; a Windows 2012R2 VM running SQL Server 2012 and a Windows 2012 VM providing the IaaS components.

VMware Data Protection Advanced will provide backup services. Initially, two VDPA instances are required. Additional instances will be deployed as required to maintain a 25:1 ratio of VMs to VDPA

instances of 25:1, as suggested by the VDPA Administration Guide (page 18). All management VMs will be backed up daily and backups retained for 90 days. Of the manufacturing VMs, only the database servers will be backed up daily and backups retained for 90 days. Other manufacturing VMs are considered "cattle" and will only hold data in transit to or from the database. These services will be redeployed in brand new VMs as necessary.

This table shows all vSphere systems and appliances and their initial resource allocations and quantities.

Service	vCPUs	RAM (GB)	System disk (GB)	Data disk (GB)	Quantity
Identity Appliance	1	2	10	0	1
vCAC Appliance	2	8	30	0	1
IaaS Components (Windows 2012)	2	8	30	0	1
VDPA	4	4	3100	0	2
vShield Manager	2	8	60	0	1
vShield Edge	2	1	0.5	0	1
vShield Endpoint	1	0.5	512	0	6

Additional RHEL VMs are required to complete the management system. The automation and orchestration system require Kickstart, Puppet Master, Gitolite, and Jenkins CI VMs (see Puppet System). Only one of each server is required to complete the system. The Puppet Master may have scaling issues if it needs to support over 1000 VMs, at which point additional master systems would need to be created. Puppet includes no built-in synchronization methods when there are multiple masters and this would introduce unnecessary complexity if it was not needed. The number of masters will be revisited after 30 days and adjusted if necessary. This table shows these VMs and their initial resource allocations and quantities.

Service	vCPUs	RAM (GB)	System disk (GB)	Data disk (GB)	Quantity
Kickstart	1	0.5	100	0	1
Puppet master	4	8	100	0	1
Gitolite	2	8	500	0	1
Jenkins CI	2	8	500	0	1

Manufacturing System

The manufacturing system has been developed by the Foundation. It is a three-tiered system consisting of a Web Front End (nginx), a Message Queue tier (RestMQ), and a Database tier (MongoDB). This system is designed for high scalability to support ever-larger starship designs, thus it will require a Load Balancer to manage connections to the various VMs at each tier. There are also two Monitor (watchdog) VMs that monitor system load and control how many VMs are deployed at each tier. Each VM has a specific resource allocation. The watchdogs will monitor utilization and create or destroy VMs as needed to maintain services levels. There is no defined upper bound but there is a minimum of two service and one load balancer VMs per tier.

THE FOUNDATION

The manufacturing process relies on continuous integration and continuous deployment processes to improve the system outputs and correct errors through rapid code deployments. In order to ensure these rapid deployments do not have an adverse effect on the manufacturing process, Development adheres to a strict change control process that involves three environments: Development, QA, and Production. Any change must be promoted upward through each environment and test successfully before promotion to Production. Any code issues or oversights are caught before the production manufacturing equipment is tested.

To achieve this goal, the vSphere cloud must deploy the manufacturing system three times in these environments. This table shows the VMs and their initial resource allocations, plus per-environment and total quantities.

Service	vCPUs	RAM (GB)	System disk (GB)	Data disk (GB)	Quantity
Web Front End	1	1	50	0	6
Message Queue	1	2	50	0	6
Database	2	4	50	200	6
Watchdog	1	0.5	50	0	6
Load Balancer	1	4	50	0	9

The cumulative totals of vCPU, RAM, and disk allocations and VM count for the initial turn up are:

vCPUs	RAM (GB)	Disk (GB)	Quantity
89	328	12833	50

THE FOUNDATION

vCAC Portal

The vCAC system components are installed according to the VM Design section. The vCAC portal allows authorized users (vSphere admins, manufacturing application developers, and certain high level Foundation officers) to provision numerous objects types ("X as a Service"). Day One blueprints in the Service catalog will include all of the standardized templates for the existing VMs (see VM Design), Active Directory objects and actions (new users, reset password, etc.). In addition, vCAC offers a REST API that allows the Foundation manufacturing system to interact with vCAC in an automated fashion.

vSphere admins will have the ability to manage the vCAC catalog, adding and updating entries as appropriate. Developers will NOT have the ability to update the catalog, as Puppet will be used to determine the correct application load out for each VM (see Puppet System), and will program the manufacturing system to use the REST API to provision objects as needed.

Management VMs will be restricted to vSphere admins only and can be deployed in any environment/network. Manufacturing VMs are restricted to developers and can be deployed in any of the manufacturing environments/networks (initially Development, QA, Production).

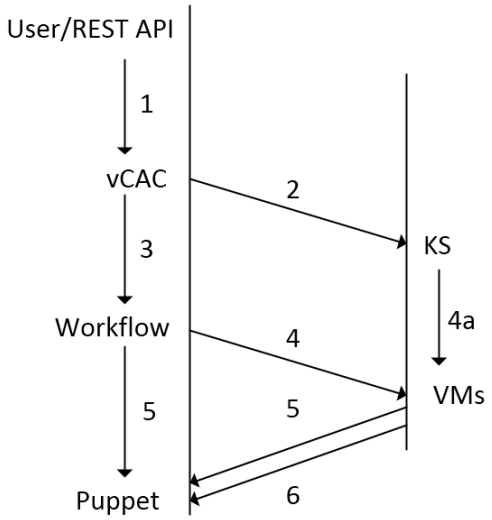
vCAC will rely upon vCenter templates (Windows), kickstart processes (RHEL) and Puppet services to provision new VMs. Other objects will rely on various service specific to the object type, such as ADS for user services.

Puppet System

The Puppet Configuration Management (CM) product is at the heart of the automation and orchestration engines and the manufacturing continuous delivery/continuous integration processes. The Foundation has chosen Puppet Open Source based on its popularity and familiarity to our personnel, and because of the well documented features and modules that allow it to manage both Windows and Linux VMs (or nodes). Puppet allows the developers to define the desired state of the node and ensure that state is achieved without worrying about how to get there.

Because Puppet applies a desired state to a system, it can start with a bare-bones template and add the required configuration during provisioning. This allows the use of a single Windows VM template per OS level (2012 and 2012R2) and the kickstart of all RHEL VMs. Node definitions can be adjusted and very rapidly, Puppet will bring all of the desired nodes into compliance with the new desired state. This "infrastructure as code" process allows for rapid code development and rapid application deployment.

All system provisioning requests (Windows or Linux) will be made through vCAC. When the user selects a VM via the catalog (see vCAC Portal for more information), vCAC will initiate a workflow to provision the VM.



1. User interactively selects or automated systems submit a REST API query for an item in the catalog and submits the request.
2. vCAC creates the kickstart file for provisioning (Linux only) and deposits it on the Kickstart VM.
3. vCAC initiates the VM provisioning workflow
4. The workflow builds the VM from template (Windows) or creates an new VM of the correct size (Linux)
    a. (Linux) The VM receives a kickstart file and downloads/installs the appropriate files.
5. The workflow forces the VM to register with puppet and signs the certificate [(ref)].
6. The vCAC workflow forces the new VM to check in to Puppet and receive its initial setup.
7. vCAC repeats steps 2-6 for any additional VMs required by the selected catalog entry.
8. vCAC notifies the requestor the catalog request has been fulfilled.

THE FOUNDATION

The vSphere administrators are responsible for configuring vCAC, the Kickstart server, the vCAC workflows, and ensuring communication between all components shown above.

The Kickstart server provides RHEL system contents for newly provisioned VMs, plus the kickstart file for the new VM. Each RHEL VM receives nearly the same basic kickstart file, only the node elements such as networking vary. Any two provisioned VMs will start with the exact same minimum level of software required to run Puppet.

The vCAC workflows communicate between vCAC, Kickstart, and newly provisioned nodes. The vSphere administrators and the developers work together to create the proper workflows.

The vSphere administrators will manage the puppet master instance(s) and the puppet code for management VMs. The developers will manage the puppet code for all remaining VMs. Both groups will provide oversight and assistance to each other, ensuring basic sanity checks and adherence to process, which ensures the manufacturing SLA (99.99%) is maintained.

Developers are responsible for aligning the puppet code with manufacturing releases. The puppet code determines the system configuration performed during provisioning step #6. The vCAC catalog will allow selection of a number of environments, including Development, QA, and Production, and developers are responsible for ensuring the Watchdog services provision in the correct environment.

All code changes also involve the Gitolite and Jenkins CI VMs. Gitolite is the authoritative version control source for all Git repositories. Developers will have their own Git workspaces, but only Gitolite and the RDP servers are backed up by VDPA. Jenkins CI is a Continuous Integration tool that is used to test changes to the manufacturing application code. The development workflow defines that all code must be tested by Jenkins CI and pass all tests to be merged upstream. This includes both puppet and manufacturing code, further validating code before deploying to any environment and assisting in maintaining the 99.99% SLA.

vSphere administrators will also follow the Gitolite/Jenkins CI and Dev->Production workflow when modifying puppet code for the management systems. Puppet will also be used to ensure a consistent state and make changes to vCenter. Developers will provide assistance as needed.

The threat from Zeds to humanity's very survival is real and the manufacturing capabilities of the Foundation are vital to reducing that threat. The use of Dev->Production promotion ensures that all changes, even those rapidly required to adapt to future manufacturing requirements, are thoroughly vetted for software bugs AND material output quality before being introduced to Production. The potential for outages can never be eliminated but combined with other availability measures, the possibility continues to reduce to a near-0 value.

THE FOUNDATION

VMware Datacenter Design

The Foundation's vCenter server will define one datacenter for Terminus City. A single cluster of 6 UCS ESXi hosts will be provisioned immediately. The cluster can scale up to 32 ESXi hosts as need grows without reconfiguration. If additional ESXi host are required, ESXi hosts will be distributed evenly into three clusters that support the three environments (Dev/QA/Prod). The cluster can also scale down once needed to a minimum viable level of 4 UCS hosts to maintain the minimum number of Management and Manufacturing VMs for the anticipated workloads.

To meet the 99.99% SLA, the cluster(s) will be configured with High Availability (HA) and Distributed Resource Scheduling (DRS). Due to the homogenous hardware stores acquired by the Foundation, Enhanced vMotion Capability (EVC) is not required at this time.

EVC cannot be changed to a lower CPU compatible mode on a running cluster and the Foundation is more likely to acquire older CPUs than newer, given humanity's current state, and EVC settings would need to be set very conservatively to future-proof the cluster against this likelihood. If this need did not arise, cluster performance and manufacturing capabilities would be impaired without justification. Both alternatives introduce risk. The probability that EVC is required is judged to be sufficiently low that the risk to manufacturing output is higher. If future iterations of the design require EVC, risk can be mitigated and manufacturing output conserved providing the current homogenous system to a colony ship and implementing a replacement heterogeneous system in the manufacturing facility.

HA will have an initial admission control policy of 7% of cluster resources to provide for 1 host failure (1/6 * 100) and will be revisited every 30 days as manufacturing capacity increases and cluster size varies. Host Monitoring will be enabled with the default VM restart priority (Medium) and Host isolation response (Leave powered on). Critical VMs will have their restart priority increased. VM Monitoring will be disabled initially. The Monitoring settings will help avoid false positives that could negatively affect manufacturing and violate the SLA. They will be revisited within 24 hours of any HA-related outage to determine if changes are required to continue to meet the SLA, and again at the 30, 60 and 90 day marks.

DRS will be configured as Fully Automated and to act on three star recommendations or greater. This will ensure the vSphere loads remain balanced across ESXi hosts as the manufacturing system scales itself. DRS rules will help ensure availability of management VMs with multiple instances.

THE FOUNDATION

A summary of initial HA and DRS rules are in the table below.

Rule Type	VMs
DRS VM-VM Anti-Affinity	DC1, DC2
DRS VM-VM Anti-Affinity	RDPLicense01, RDPLicense02
DRS VM-VM Anti-Affinity	RDPSH01, RDPSH02
DRS VM-VM Anti-Affinity	RDPSH03, RDPSH04
DRS VM-VM Anti-Affinity	RDPSH01, RDPSH04
DRS VM-VM Anti-Affinity	VDPA01, VDPA02
DRS VM-VM Anti-Affinity	DevWatchdog01, DevWatchdog02
DRS VM-VM Anti-Affinity	QAWatchdog01, QAWatchdog02
DRS VM-VM Anti-Affinity	ProdWatchdog01, ProdWatchdog02
VM Override VM Restart Policy - High	Management - vCenter, DCs
VM Override VM Restart Policy - High	Automation - Identity App, vCAC App, Gitolite VM
VM Override VM Restart Policy - High	Manufacturing - Database and Watchdog VMs
VM Override VM Restart Policy - Low	Web Front End VMs

THE FOUNDATION

Security Architecture

The security of the manufacturing security is extremely vital. Any security compromises, accidental or purposeful, risk the entire human race. Defense in depth (or layers) will mitigate nearly all security gaps.

> ***Security is an ongoing concern and the steps outlined here define an initial security policy only. The architecture, policy, and implementation will immediately and continually evolve to meet the demands of the system and its users. Therefore this document is NOT be considered authoritative for the production system.***

All VMs will use the OS's included host firewall (Windows Firewall or iptables) to manage inbound traffic. The template VMs will include a very conservative policy (inbound ssh and established connections only) and the puppet manifests will manage additional rules for each VMs installed applications. Outbound VM traffic will not be managed with host firewalls unless an application specifically calls for it (currently none do).

Inter-VLAN traffic will be managed and protected with VMware vCloud Networking and Security 5.5.2. vShield Manager, vShield Edge and vShield Endpoint will provide central management, protection between networking segments, and in-VM protection from viruses and malware. vShield App is not required due to Guest OS firewalls and vShield Data Security is not a relevant concern to the isolated VMware cloud.

The system's edge, between the manufacturing network and the Foundation's LAN/WAN, will be protected with a Fortigate-300C in routed, single-VDOM mode. The FortiGate license allows for multi-VDOM mode (multiple logical firewall instances per interface/VLAN) if necessary in the future. Initial policy will allow unrestricted outbound common services and more restricted inbound services according to the table below.

Manufacturing to Foundation LAN/WAN			
SRC	DST	SERVICE	ACTION
Internal Networks	External Networks	http, https, ssh, smb, dns	Permit
Foundation LAN/WAN to Manufacturing			
SRC	DST	SERVICE	ACTION
vSphere Admins	vCenter	9443/tcp	PERMIT
vSphere Admins, Developers	Puppet System	ssh	PERMIT
vSphere Admins, Developers	RDP Session Hosts	rdp	PERMIT

vCenter SSO will use the Active Directory domain as the primary namespace. All vSphere administrators and the chosen colonist will be in the Administrator group. Developer team leads will be in the Power User role. Other developers will have read-only access unless specifically requested and granted. The administrator@vsphere.local account information is made known to the vSphere team lead and the colonist (prior to launch) in order to reduce the potential for unaudited actions that could cause harm.

THE FOUNDATION

The ESXi hosts will have lockdown mode enabled. The local root account password will be shared with all hosts (applied via host profile) and will be made known to the vSphere team lead and colonist (again prior to launch) in case local DCUI/shell access is required.

Monitoring and Capacity Planning

The Foundation has no existing workload to evaluate for capacity planning. vSphere administrators will review the vCenter performance graphs for both real-time monitoring and basic historical analysis/trending.

Day one monitoring will consist of vCenter's default alerts. vCenter alerts will be configured to send email notification to the vSphere administrators as well as the manufacturing plant's on-shift manager and a designated military liaison. Notification to three parties will ensure that alert responses are timely. After workloads are in place for five days and the vSphere administrators have a baseline utilization to reference, the alerts will be customized. A balance between too much alerting, which breeds complacency and ignorance, and too little alerting, which may result in outages or impacts occurring, must be maintained.

The lack of existing baselines and the extreme urgency of immediate manufacturing prevents more accurate forecasting of monitoring and capacity planning needs. Ongoing management of the infrastructure and humanitarian efforts may preclude vSphere administrators having excess time to manage a monitoring system, especially if the workloads are stable and within thresholds. However, vCenter Operations Management Suite has been procured and, time and effort permitting, will be installed and configured within the next 30 days to provide enhanced monitoring and capacity planning.