CHALLENGE 2 – NO CLOUD IN SIGHT

(A NEW PUBLIC CLOUD)

BY JAMES BROWN (@JBCOMPVM)

Contents

Executive Summary

The Infrastructure team has been tasked by the billionaire philanthropist to suggest a public cloud service that was running on Earth, which can be built on Mars. Once the public cloud service has been suggested, a solution design must be completed. A single webserver needs to be created to track time within the greenhouse. An enterprise application needs to be built to run the live support system. No application requirements have been establish. According to the EVIL Sectary of State, Melissa, we need to design these applications without specification and lack of existing baselines. Performance, capacity, latency, and high availability needs to be thoroughly developed.

Requirements

1. Applications must run in a public cloud environment
2. Each colony must be capable of working fully independently.
3. A minimum of three additional datacenters are planned.
4. Greenhouse systems need to be available at all time.
5. Greenhouse systems will utilize Linux and MySQL.
6. Support Service are mission critical. Without these services the human race will not survive,
7. The design must be highly reliable and easily deployable.
8. Performance, capacity, latency, and high availability need to be developed

Constraints

1. Power, cooling, and space are very expensive resource. They needed to be used sparingly.
2. The design must incorporate the use of reliable, serviceable technology that can degrade gracefully over time.

Assumptions

1. There are three data centers
2. All specified hardware and software can be acquired and will work on Mars.
3. Authentication will be handled from Windows Active Directory
4. Data center connections are 40 GB with QinQ enabled.
5. Appropriate licensing for all vendor products (VMware, Microsoft, Red Hat, etc.).
6. vSphere administrators have and can maintain the skillsets required to implement and maintain the solution.

Risks

1. Cloud environment has not be built on Mars
2. A lack of appropriate personnel may jeopardize the ability to maintain and improve the environment.
3. No existing matrix to evaluate or use for capacity planning.
4. Unknown specification for the time tracking web application
5. Unknown specification for the support system enterprise application

Conceptual Design

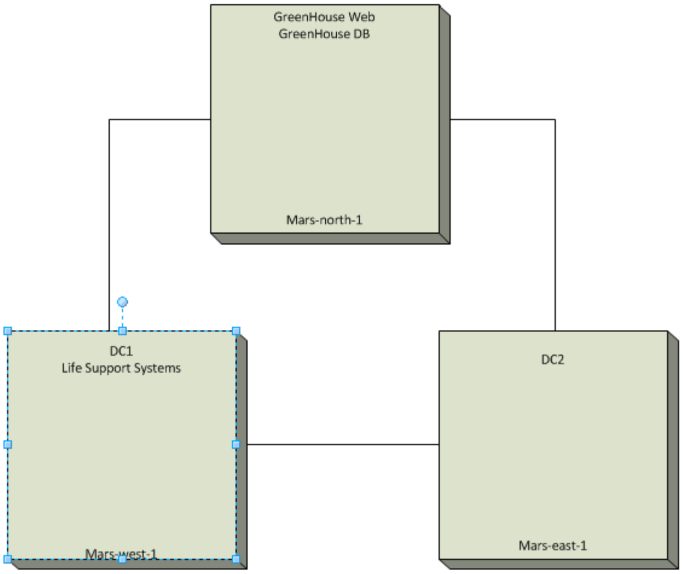
Choice of Public Cloud

From the first challenge we know that there are three data centers on online Mars. Our billionaire philanthropist has tasked the design team to recommend a public cloud service that was operational on Earth to build out on the Mars colony.

Amazon Web Services (AWS) was the number one public cloud provider before the zombies decided to eat the human race. AWS has the ability to customize to any number of desired applications and workloads.

Services are:

1. Compute
2. Storage & Content Delivery
3. Database
4. Networking
5. Administration & Security
6. Analytics
7. Application Services
8. Deployment & Management
9. Mobile Services
10. Enterprise Applications



Three data centers will be created. The names are as follows:

mars-north-1

mars-west-1

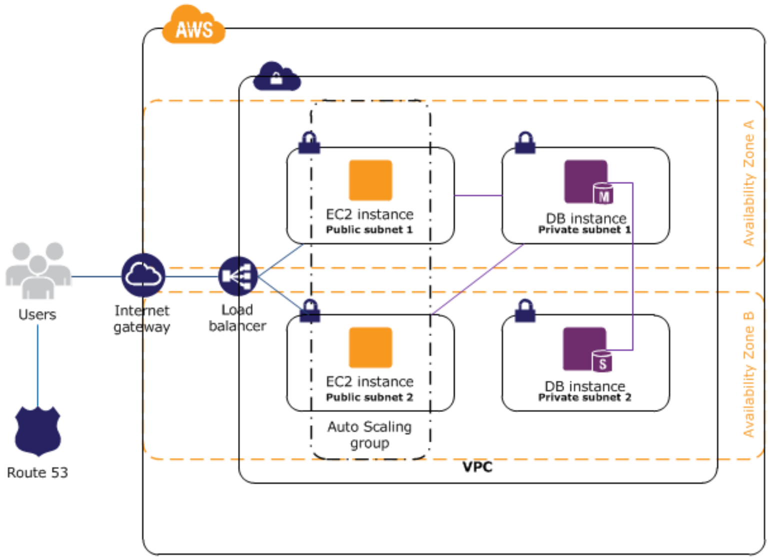
mars-east-1

Architecture

Web Application

This application server will control the time tracking software for the green house.

This is the logical design for the green house webserver



Required AWS Services:

AWS Service	Instant Type	Region	Machine Image
EC2	m3.large	Mars-north-1	RedHat
RDS	db.m3.xlarge	Mars-north-1	mySQL
LB		Mars-north-1	

Image and documentation on

http://docs.aws.amazon.com/gettingstarted/latest/wah-linux/web-app-hosting-intro.html

Because of the critical nature of the Green House we are creating a highly available webserver with a backend database that is also replicated.

VPC availability zones will be used. VPC allows you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. These two VPC availability zones will have a load balancer to provide reliability. User will access the webserver from the internet through a public URL, e.g. https://thegreenhouse.mars.gov

Linux and MySQL are being used for developer requirements.

M3.large has 2 vCPU and 7.5 GB of memory

Db.m3.xlarge has 4 vCPU and 15 GB of memory

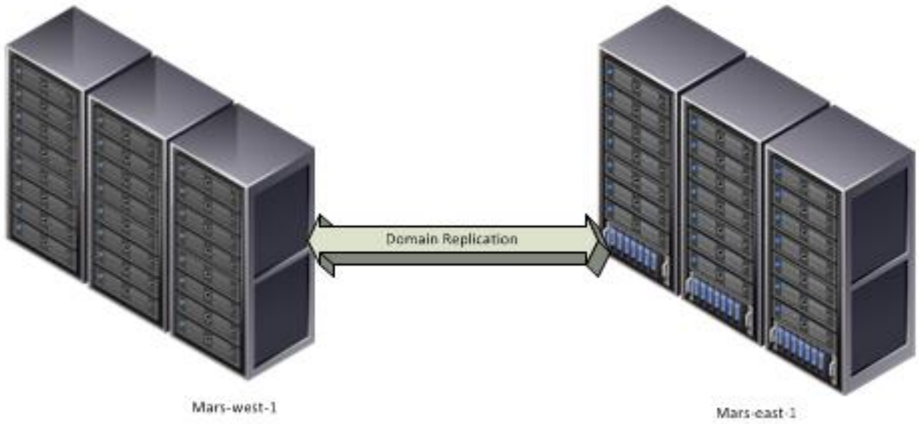
Windows Domain

General network and end user access will require integration with new or existing Active Directory forest. A new domain and forest will be created and two Windows 2012 R2 will be provisioned as domain controllers. Windows 2012 R2 Datacenter licenses have been acquired and all additional Windows guests will also run 2012 R2 unless otherwise specified.

Domain controller are not resources intensive. Three domain controller will provide redundancy and failover capibilities

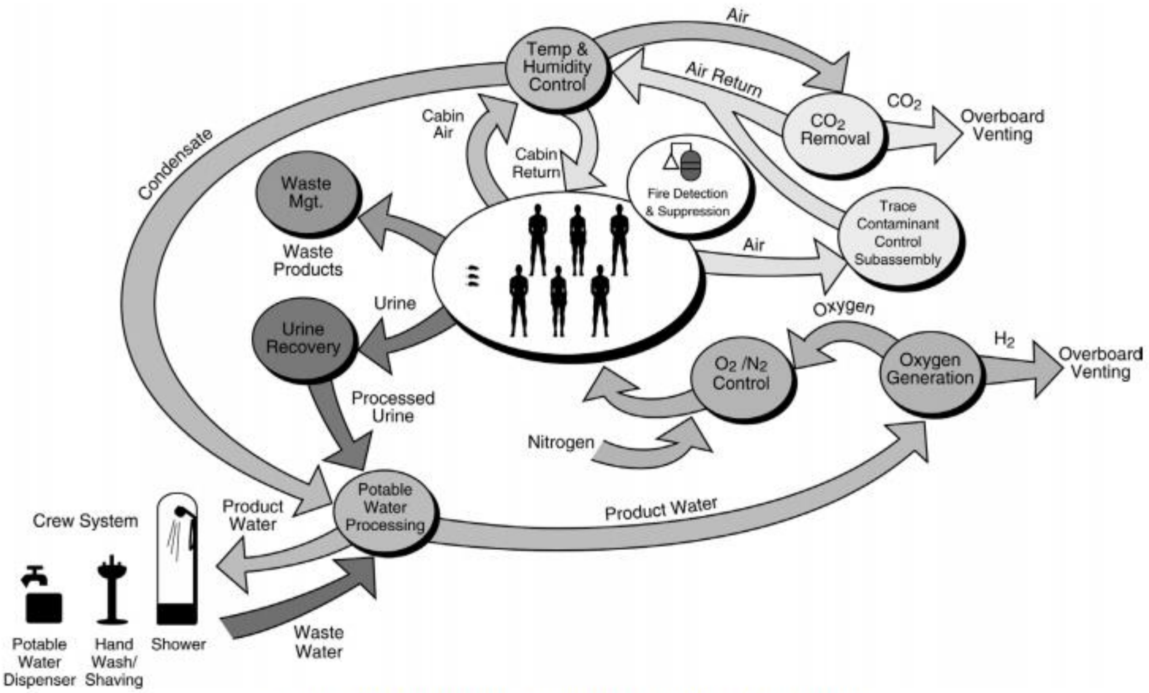
These domain controller will be built with the t2.medium instance type. This instance includes 2 vCPU and 4 GB of memory. AWS EBS is used for storage. Network performance is low to moderate. It is highly recommend that the domain controller be in separate regions.

The local domain for the support and greenhouse with be mars.col



Business Critical application – Life Support system

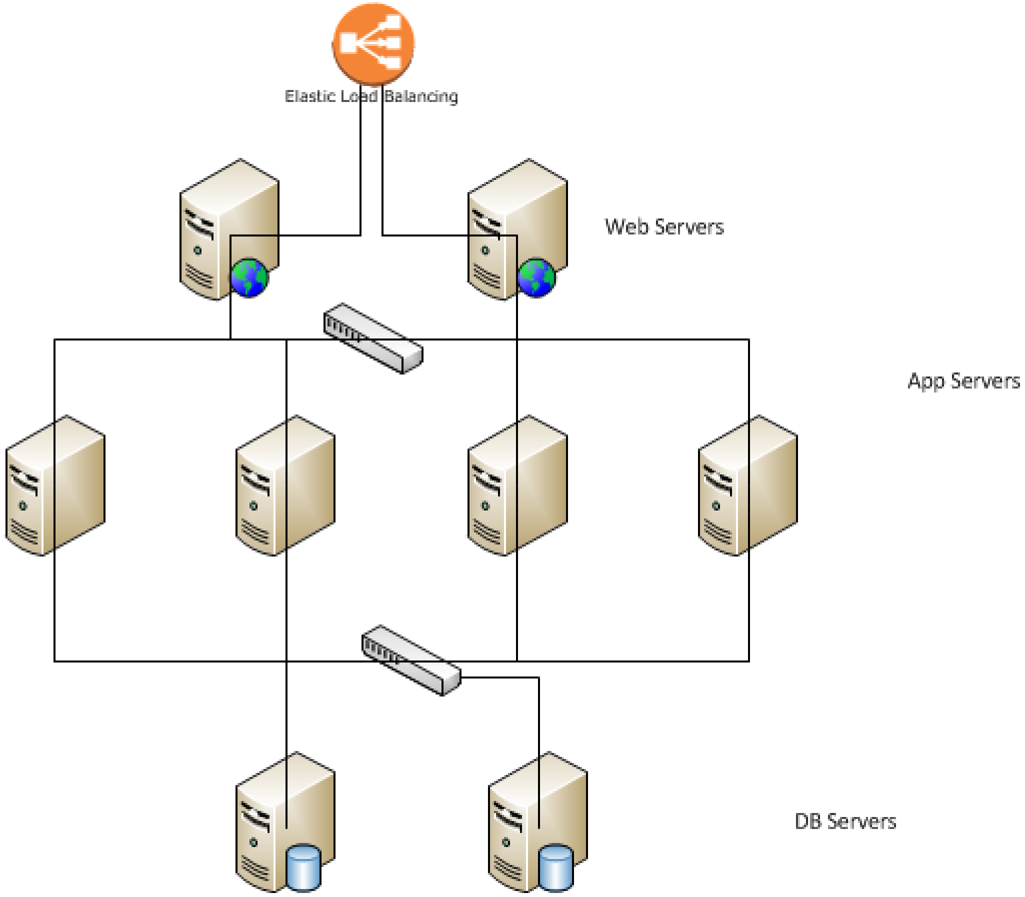
The life support system is the most critical system of all. Without this system the human race could not survive on Mars. The image below show the major systems within a life support system.



Regenerative Environmental Control and Life Support System Diagram

The follow systems will require an AWS Instance:

- Management Server (Webserver)
- Waste managements (Urine recovery and water processing)
- Oxygen generation
- Temp and Humidly control
- 02 and N2 Control
- All servers will connect to a redundant DB server


Elastic Load Balancing
Web Servers
App Servers
DB Servers

Server	AWS Service	Instant Type	Region	Machine Image	Storage (GB)	IOPS
Load Balancer	LB		mars-west-1			
Management1	EC2	m3.large	mars-west-1	Windows 2012 R2		
Management2	EC2	m3.large	mars-west-1	Windows 2012 R2		
Waste Management	EC2	m3.large	mars-west-1	Windows 2012 R2		
Oxygen Generation	EC2	m3.large	mars-west-1	Windows 2012 R2		
Temp and Humidity Controls	EC2	m3.large	mars-west-1	Windows 2012 R2		
O2 and N2 Control	EC2	m3.large	mars-west-1	Windows 2012 R2		
DB Server 1	RDS	db.m3.xlarge	mars-west-1	MS SQL Enterprise	400	3000 (SSD)
DB Server 2	RDS	db.m3.xlarge	mars-west-1	MS SQL Enterprise	400	3000 (SSD)

The webservers will be in a HA/load balanced configuration.

- URL https://supportsystems.mars.gov

All application servers will support their respective application.

The DB servers will be setup in an AlwaysOn Failover Cluster.

All servers will be setup on the mars-west-1 region. We will utilize Cross-Region Replication for all the support systems. System on mars-west-1 will be setup to replication to mars-east-1. If a region is offline for a long period of time, an AWS administration will have to setup replication to mars-north-1 manually.

Backup

Skeddly will be implemented to created automatic daily backups. Skeddly will create backups for EC2, RDS, and load balancers.

http://www.skeddly.com/snapshots/

Security Architecture

The security of the green house and support systems are vital. Any security compromises, accidental or purposeful, risk the entire human race.

Security is an ongoing concern and the steps outlined here define an initial security policies. 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 AWS instances will use the OS's included host firewall (Windows Firewall or iptables) to manage inbound traffic for the provided services and administrative management only.

The following system will be joined to the mars.local domain

- Waste Management
- Oxygen Generation
- Temp and Humidity Control
- O2 and N2 Controls
- DB Server 1
- DB Server 2
- Management1
- Management2
- DC1
- DC2
- DC3

Security and GPO policies will be enforced by the System Administrators. These policies will evolve as we continue to thrive on Mars.

Monitoring and Capacity Planning

The Mars colony has no existing matrix to evaluate or use for capacity planning. AWS administrators will review the Netflix Ice performance graphs for both billing and usages. Based on these finds, changes will be made to the AWS instance to increase or decrease capacity, latency, and performance.

The lack of existing baselines prevents more accurate forecasting of monitoring and capacity planning. Ongoing management of this new public cloud infrastructure and other efforts may preclude AWS administrators having excess time to manage a monitoring system, especially if the workloads are stable and within thresholds. Training and staffing levels will need to be monitored on a monthly basis.

Revision History

Date	Revison Number	Author	Comment
9-Jul	1	J. Brown	Start the Design
11-Jul	1.1	J. Brown	Finalized draft 1
12-Jul	1.2	J. Brown	Design comments and grammar issues pointed out by Rob Nelson