Virtual Design Master

Conceptual Design
Challenge 2

Prepared by
Dennis George

Authors

The following authors contributed to the creation of this deliverable.

Dennis George
892 Bessy Trail, Milton, ON L9T 0A6 Canada (905) 699 – 3151 dennisgeorg@gmail.com

Revision History

Revision	Change Description	Updated By	Date
0.1	Document Created	Dennis George	07/08/2015
0.2	Document Updated	Dennis George	07/09/2015
0.3	Document Updated	Dennis George	07/10/2015
0.4	Document Updated	Dennis George	07/11/2015
0.5	Document Updated	Dennis George	07/13/2015
0.6	Final Deliverable	Dennis George	07/13/2015

Table of Contents

SECTION 1: OVERVIEW

Executive Summary

Project Overview

Millionaire philanthropists Richard M. and Elon B., have teamed up to work towards humanity's survival after the outbreak of the virus, that lead to the zombie apocalypse and evacuation of what was left of the human species from earth. They are seeking an infrastructure design for permanent human colonization in Mars. Virtual Design Master an online reality show that challenges virtualization professionals to come up with innovative virtualization designs has been tasked to select the next Virtual Design Master to design a permanent IT infrastructure in Mars.

In challenge 1, the team designed an "on-prem" infrastructure solution to support various critical control systems such as the Environmental system, Greenhouse control system, and productivity and collaboration systems.

As part of the challenge 2 initiatives, the team is tasked to design a solution to support the same requirements in a public cloud of choice and provide justification for the same.

The Conceptual Design provides a high-level overview of the proposed solution for the "Cloud First" strategy that the team has been tasked with. The team has chosen Amazon Web Services (AWS) as the cloud services provider of choice, and this design deliverable outlines "Phase 1" of the design which leverages two AWS regions, each with two availability zones, to provide redundant infrastructure services for our two mission critical applications "Time Warp" and "The Oracle", including BCDR capabilities.

Also, in order to satisfy data sovereignty and data governance constraints imposed by the mission critical life support system, the design leverages Equinix, a Tier-1 datacenter colocation facility, NetApp Private Storage for AWS, and 10 Gb AWS Direct Connect link to the AWS cloud.

Furthermore as an outcome of this engagement, "Phase 2" and future vision of the design has been defined, as the team has learnt that the long-term strategy for the Mars base IT infrastructure is going to be hybrid-cloud based due to data governance and sovereignty requirements, and the solution should plan for an enterprise automation and orchestration framework that is cloud-agnostic such that "XaaS" offerings from different cloud service providers can be leveraged, and the solution should also integrate with the enterprise "on-prem" design that was delivered as part of Challenge 1. "Phase 2" of the design will be tackled as part of future engagements.

Both applications introduce specific requirements around availability, performance, security, latency and capacity. "Time Warp" is a web-based time tracking application for the botanists in the greenhouse, which is an application based on the LAMP stack, and "The Oracle" is an enterprise .Net based windows application which monitors critical life support systems for the Mars base, such as production of water and oxygen as well as reclamation of waste.

As part of the design, an application delivery solution comprising of Citrix XenApp along with the Citrix NetScaler Application Delivery Controller was chosen, providing Global Server Load balancing across AWS regions and availability zones and service load balancing, within each availability zone, unified, device-agnostic and secure enterprise and web application access using Multifactor Authentication, and Single-Sign On.

Project Goals

During the course of the project, the Virtual Design Master team and Dennis George identified a number of different project goals. The following summarizes those goals and illustrates how this Conceptual Design deliverable addresses them.

Priority	Key Characteristics	Description
1	Minimize utilization of Power, Space and Cooling for the new infrastructure.	The design leverages the AWS public cloud service, with auto-scaling of instances to scale up/down services to meet application needs as well as minimize Power and Cooling requirements.
2	Limit design to 10G and 40G switching gear. In order to save on space, the design should not use Fibre Channel switching.	The design does not require any switching equipment since the solution leverages public cloud services. Data Sovereignty requirements introduce a constraint, which imposes requirement for business owned storage subsystem to be co-located at partner datacenter co-location facility.
3	Critical applications such as Environmental system, Greenhouse control system, and Communication systems should be made highly available	All critical systems will be made highly available across cloud datacenter facilities (AWS Delivery Zones) to provide HA and geographically dispersed cloud datacenter facilities (AWS Regions) for BCDR. In addition enterprise Web Applications and Windows Applications will be delivered using Citrix XenApp and Citrix NetScaler appliances providing Global Server Load balancing services across the AWS Delivery Zones, an AWS Regions.
4	The design should be able to support an unknown business critical application in the future.	The design leverages Amazon Virtual Private Cloud (VPC), which provides for logical segregation of individual IP subnets etc., such that future “unknown” applications can be integrated with ease.
5	Meet requirements of the Time Tracking and Life Support Systems Applications as	All requirements outlined by the applications have been met as part of this design deliverable.

Application Requirements -“Time Warp” - Time Tracking Application

Overview

The Botanist who work in the Greenhouses use a Time Tracking application call “Time Warp” which is a critical component of their work day.

“Time Warp” is a web-based time tracking application used by the botanists in the greenhouse. The application is based on scale-out LAMP stack, consisting of PHP based application running on Apache Web Server, a “Memcached” caching engine, and a MySQL Database.

Requirement ID	Description
APP01REQ01	**Performance** - Being a user facing application, it is imperative that it performs well even during surges of user activity. The botanists in the Greenhouses are very busy, and lost time could even mean pods loosing upto 50% of oxygen recycling capabilities.
APP01REQ02	**Availability** –The availability of the time tracking application for the botanists is imperative, without which the Botanists will not go to work, as they feel they are already underpaid and overburdened.
APP01REQ03	**Latency** – The botanists are usually mobile, moving from one Greenhouse to the other, and they do not have good Wi-Fi connectivity while on the move, which means lower bandwidths and higher latencies. They should be able to log time as they commute with good user experience even while they are on the road without hampering their productivity.
APP01REQ04	**Capacity** – Robust Load balancing of the Web application tier is required, with intelligent health monitoring and the ability to automatically Scale-up/down based on environment demands.
APP01REQ05	**Scale-out Caching Tier** – The application leverages Memcached in the caching tier, and is requirement for speedy application execution. An easy to deploy scale-out Memcached service should be available.
APP01REQ06	**Single Sign-On (SSO)** - The end-user should be able to access all their Enterprise applications by Signing-in only once.
APP01REQ07	**Secure Remote Access from any device** – The access to this application should be secure, both for data-at-rest and data-in-motion.
APP01REQ08	**Service monitoring and visibility** – Real-time service monitoring and notification capabilities is requirement for the IT staff to quickly be notified of any service issues.

Application Requirements – “The Oracle” - Life Support Systems Application

Overview

Humanities existence on Mars is dependent on the availability and performance of critical application that supports Life Support Systems on Mars. This is a suite of Windows Services called “The Oracle” that services, and monitors the Life Support Systems for mechanical failure and provide proactive alerts to facilities personnel. The Life Support Systems maintained by this suite of applications are Water and Oxygen production and also reclamation of waste. This application suite needs to be geographically close to these Life Support systems, with high-bandwidth low-latency connectivity to service and monitor these critical systems.

The application also has a Windows based thick client application that needs to be made available only to personnel with “Top Secret” security clearance, on any device of their choice,

“The Oracle” also represents a unique Data Sovereignty challenge for Data-At-Rest and Data-In-Motion as outlined before, wherein the application and all its components and data has to be stored on storage that is owned by the business, and should not be stored on Public Cloud storage.

Requirement ID	Description
APP02REQ01	**Availability** – The availability of these critical Life Support systems is important for the survival of the human race in Mars. The failure of these systems can only be sustained for 20 minutes.
APP02REQ02	**Security** – Security is a very important concern when it comes to the Life Support Systems, hence Multi-factor authentication should be enforced to validate user identity,
APP02REQ03	**Performance** – The Life Support Systems are CPU intensive and hence the platform should be able to monitor key performance metrics and automatically scale-up the environment based on capacity requirements.
APP02REQ04	**Latency** – The Windows Services backend needs to have low latency, high bandwidth connectivity to the facilities housing the Life Support systems in order to properly support the mechanical systems and deliver timely alerts for impending failure.
APP02REQ05	**Data Governance and Sovereignty** – All applications, components and associated data for this suite of applications should be stored only on business owned storage, with stringent access restrictions, while being able to leverage the public cloud for execution of these workloads.
APP02REQ06	**Monitoring** – Watch dog processes generate alerts on impending mechanical failures, customization monitoring solution than can generate alerts on real-time triggers is required.
APP02REQ07	**Capacity** – Controlled modular growth of these Life Support Systems that maps to new Pods being built enables capacity planning. Having said that the Windows Services tier should be able to auto-scale to meet unexpected surges in CPU resources, such as during failure events.

Requirement ID	Description
APP02REQ08	**Secure Remote Access from any device** – The access to this application should be secured by leveraging encryption, both for data-at-rest and data-in-motion.
APP02REQ09	**Service monitoring and visibility** – Real-time service monitoring and notification capabilities is requirement for the IT staff to quickly be notified of any service issues.

Deliverable Summary

Supplemental Information and Links

These links provide further information on the concepts and recommendations discussed during this document.

- Mars Mileage Guide – A comprehensive guide outlining the distance between various locations on Mars.
- NetApp FAS6290 Series enterprise data storage controller - NetApp FAS6200 Series storage systems are designed to deliver superior availability and proven performance to satisfy the most demanding workloads.
- Avernus Cavi - Lake in Campania, Italy, supposed to be an entrance to the underworld.
- Boeddicker Crater - Named for: German astronomer Otto Boeddicker (1853-1937)
- Curiosity (USA) - Landed successfully. Currently in operation.
- MER Spirit Rover (USA) - Landed successfully in January of 2004, operated for just over 7 years, 4 months.
- Beagle 2 Lander (UK) - British lander, part of Mars Express mission. Failed during descent.
- Mars 2 Lander (USSR) - Failed during descent. First man-made object on Mars.
- Mars Craters – Google Maps showing location for craters in Mars.
- AWS - Regions and Availability Zones – AWS documentation describing Regions and Availability Zones.
- Amazon Virtual Private Cloud Connectivity Options - This whitepaper is intended for corporate network architects and engineers or Amazon VPC administrators who would like to review the available connectivity options.
- Equinix Cloud Exchange - The Equinix Cloud Exchange brings together cloud service providers and users, enabling them to establish affordable, private, high-performance connections within Platform Equinix.
- NetApp Private Storage for Amazon Web Services - NetApp® Private Storage for Amazon Web services allows enterprises to build an agile cloud infrastructure that balances private and cloud resources to best meet their business needs.
- AWS Direct Connect - Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
- NetApp Cloud: Cloud ONTAP for Amazon Web Services - NetApp Cloud ONTAP is a key element in NetApp's vision to create a NetApp Data Fabric that simplifies data mobility and management for the hybrid cloud. This article explains how Cloud ONTAP works in concert with OnCommand Cloud Manager software to simplify management of data in the cloud.
- Implementing Active Directory Domain Services in the AWS Cloud – This article outlines the steps involved in setting up Microsoft Active Directory Services in the AWS Cloud.
- AWS Directory Service - AWS Directory Service is a managed service that allows you to connect your AWS resources with an existing on-premises Microsoft Active Directory or to set up a new, stand-alone directory in the AWS Cloud.

- EC2Config - Seamlessly Join EC2 Instances to a Domain – Amazon utility for joining EC2 instances to a Microsoft Active Directory Domain.
- Introducing NetScaler 10 on Amazon Web Services - Citrix NetScaler 10 delivers elasticity, simplicity and expandability of the cloud to enterprise cloud datacenters and already powers the largest and most successful public clouds in the world.
- Implementing Microsoft Windows Server Failover Clustering (WSFC) and SQL Server 2012 AlwaysOn Availability Groups in the AWS Cloud –
- vRealize Automation Support Matrix – The article outlines vRealize Automation Support Matrix for different cloud technologies
- AWS ElastiCache - An AWS Public cloud Memcached service.
- Configuring Single Sign-On to Web Applications – This article outlines the steps required to configure Single Sign-On for Web Applications leveraging Citrix NetScaler Gateway.
- Google and VMware Collaborate on Enterprise Public Cloud – Article outlining future integration plans between VMware vRealize Automation and Google Public Cloud services.

SECTION 2: THE CHOSEN ONE – AMAZON WEB SERVICES

As part of the proposed design, the team has chosen Amazon Web Services (AWS) as the public cloud services provider of choice for our infrastructure on Mars.
This choice was made after careful consideration to the project requirements, and long-term vision of infrastructure services for the human settlement on Mars.

The primary drivers for selecting Amazon Web Services as the public cloud of choice are as follows:

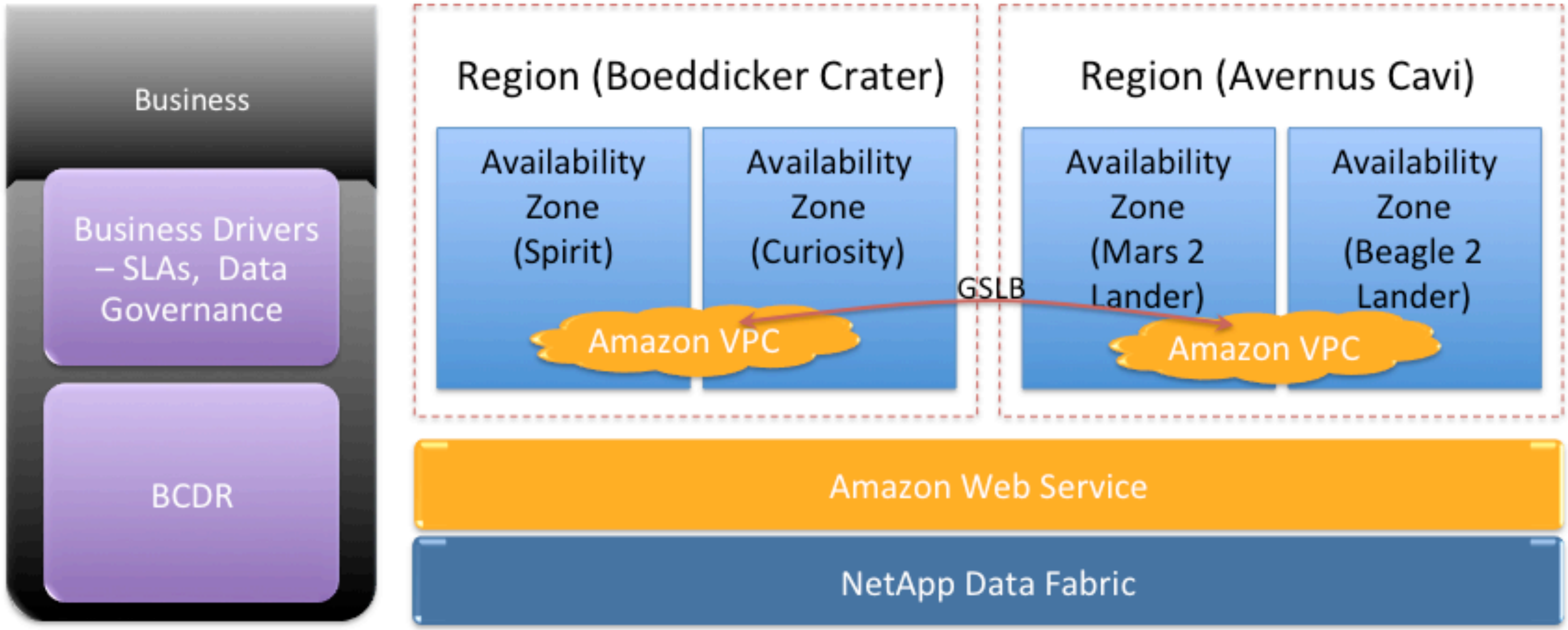
- Multiple global facilities around the world, providing numerous “Availability Zones” (datacenters) within each Region for low latency network connectivity for HA and “physical separation of resources” and also multiple “Regions” for Disaster Recovery scenarios.
- Global colocation partners to address data sovereignty concerns, while still being able to leverage pubic cloud infrastructure for everything else.
- Massive ecosystem of XaaS available when leveraging the AWS cloud.
- Most mature public cloud services platform in the market with a massive portfolio of services.

Ability to satisfy “All” requirements and constraints imposed by the “Time Wrap” and “The Oracle” applications.

SECTION 3: CONCEPTUAL DESIGN

Architecture

The following logical diagram illustrates the high-level architecture of the AWS cloud infrastructure that will be leveraged for this design.


Business
Business Drivers – SLAs, Data Governance
BCDR
Region (Boeddicker Crater)
Availability Zone (Spirit)
Availability Zone (Curiosity)
Amazon VPC
GSLB
Region (Avernus Cavi)
Availability Zone (Mars 2 Lander)
Availability Zone (Beagle 2 Lander)
Amazon VPC
Amazon Web Service
NetApp Data Fabric

- AWS Regions are completely isolated from each other, and hence will be leveraged for Disaster Recover purposes.
- AWS Regions on Mars will be located in craters, and hence will have the lowest elevation, and will provide natural cooling for the datacenters. The two AWS Regions leveraged for this design is “Boeddicker Crater” and “Avernus Cavi”.
- Each AWS Region consists of multiple Availability Zones, these correlate to datacenters. Availability Zones within a Region are connected to each other over low-latency links. Two Availability Zones per Region has been selected for this design:

Region	Availability Zone
Boeddicker Crater	Spirit
	Curiosity
Avernus Cavi	Mars 2 Lander
	Beagle 2 Lander

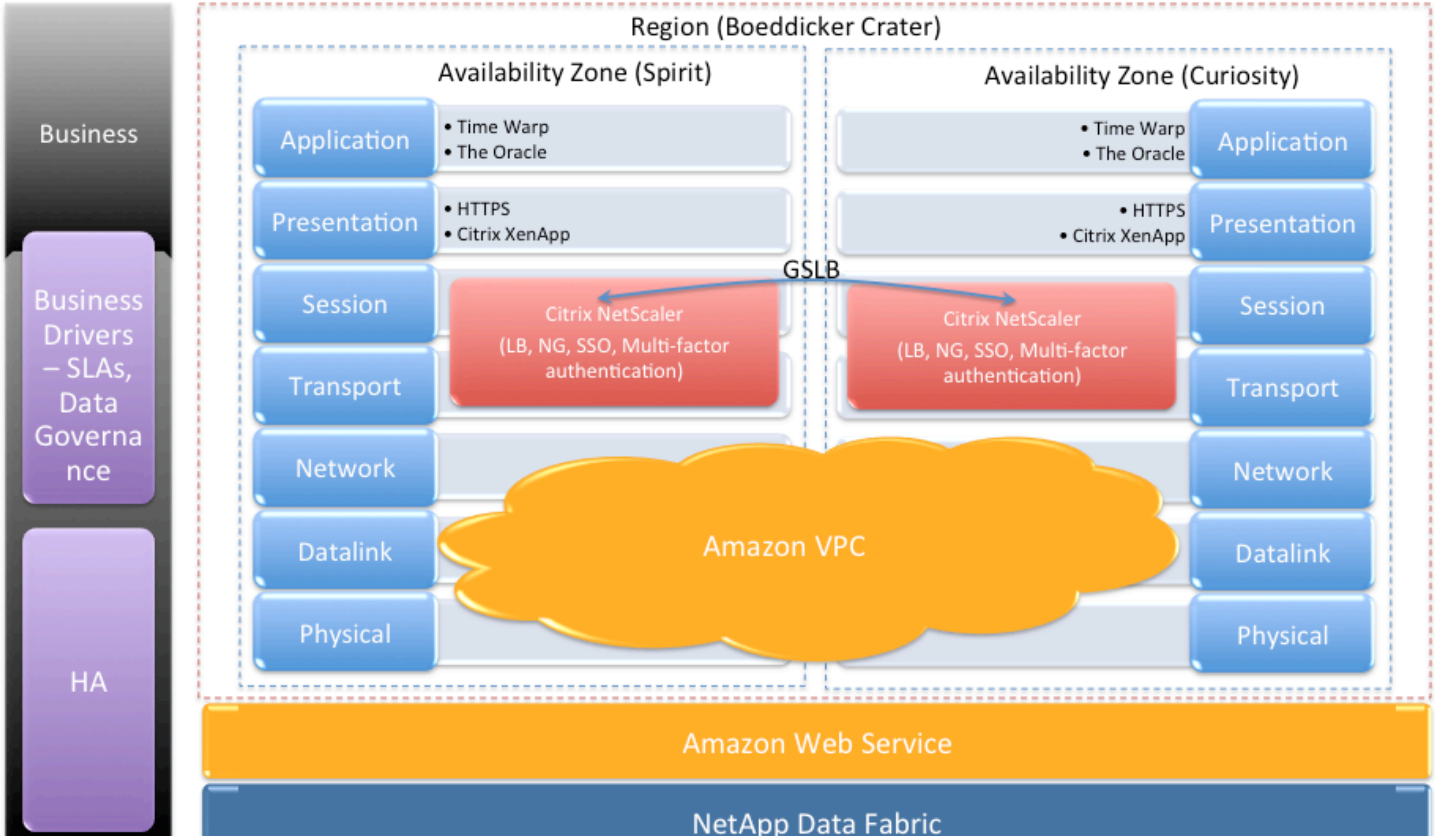
  Each of the Availability Zones is located at sites where past human missions to Mars were targeted for landing.
- The two AWS Regions will be connected via the Amazon Direct Connect and Equinix Cloud Exchange WAN backbone network for inter-region connectivity.
- Each AWS Region will serve applications and systems for “local” human pod Life Support Systems and Greenhouses. Citrix NetScaler Global Server Load balancing (GSLB) solution will “pin” Region specific user groups to local application services, and will only failover to the secondary Region incase of a disaster wherein both Availability Zones within the Region has been lost.
- One Amazon Virtual Private Cloud (VPC) will be created within each AWS Region, each spanning the two Availability Zones within the Region.
- The Availability Zones will be leveraged for High-Availability purposes but the relatively low distance between Availability Zones do not make them good candidates for Disaster Recovery, and hence different regions will be leveraged for Disaster Recovery purposes.
- The zombies have adapted, and there are rumors that some zombies could have disguised themselves as humans in the last pod of humans sent to Mars, in an effort to infiltrate the Life Support Systems in Mars to spread the virus.
  This introduces Data Sovereignty and Data Governance concerns, since the data stored in the Life Support System, “The Oracle” contains Intellectual Property, and if fallen in the wrong hands could lead to the annihilation of the human race. Hence, “The Oracle” will leverage NetApp Private Storage deployed in Equinix, a Tier-1 datacenter colocation facility built on Mars, connected to the AWS cloud using 10 Gb Amazon Direct Connect link. Access to this system will be tightly controlled using extensive screening, “Top Secret” security clearance, and Role-Based Access.
- All components of “The Oracle” application will reside on NetApp Private Storage, and replicated using Snap tools to another Equinix colocation facility in the second AWS Region for BCDR purposes. None of the components related to “The Oracle” application will leverage the AWS S3 cloud storage.
- Each AWS Region will have an instance of Cloud ONTAP, which will manage availability of data across the different Availability Zones in a Region. The NetApp Storage layer will be referenced as the NetApp Data Fabric.
  This also sets the premise for “Phase 2” of the design, which calls for a Hybrid Cloud strategy for some applications that would be need to be deployed “on-prem” for compliance purposes.
- Microsoft Active Directory Services domain named “**prometheus.net**” will be deployed as instances within AWS, comprising of two Active Directory Domain Controllers per Availability Zone, with one Global Catalog server per Availability Zone. Appropriate Active Directory (AD)

Sites and Services configuration will be performed, in order to reflect inter-availability zone and inter-region link costs to optimize AD replication traffic.

- AWS Directory Services based AD Connector will be configured to the “**prometheus.net**” domain, and leveraged for providing Role-Based Access to the AWS Console using AD Security Group membership, and for joining Windows instances to the domain.
- A custom DHCP Option set will be configured for Windows based instances, such that AD DNS services are leveraged by the machines.
- Secure remote access to both Enterprise Web applications and Windows applications on any device will be provided by leveraging Citrix XenApp and Citrix NetScaler.

AWS Region Architecture

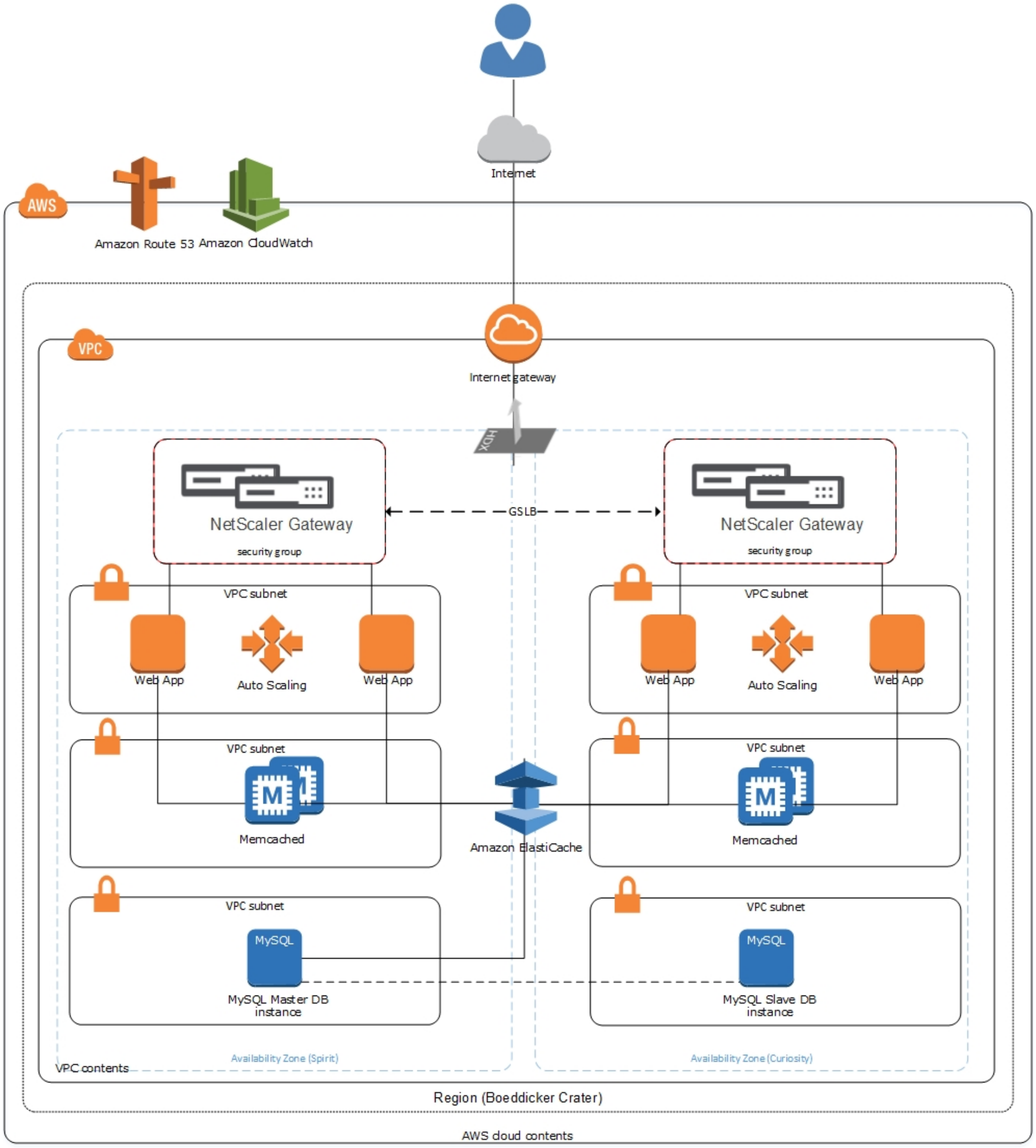
The following logical diagram outlines a single AWS Region, and the associated services provided within each layer of the technology stack:



- AWS Availability Zones are “physically” isolated from each other, and provide low-latency links between each other. Availability Zones are geographically close to each other, and hence are good candidates for providing HA services, but not BCDR.
- Each AWS Availability Zone will have the full stack of services for each of the applications in order to provide Fault Tolerance and High Availability of services in case of AWS Availability Zone failures.
- An HA pair of Citrix NetScaler VPX Platinum Edition virtual appliances will be deployed in each AWS Availability Zone, which will provide NetScaler Gateway services for secure remote access leveraging multi-factor authentication to Enterprise Applications, and SSO for Web Apps.
- Citrix NetScaler will be leveraged for Global Server Load Balancing for application access between the different Availability Zones within a Region, wherein the users will be load balanced in an active-active fashion using round-robin algorithm between the two Availability Zones. Once an application is launched by a user in any one of the Availability Zones, all future requests for the application will return to the same Availability Zone until the session expires, or the users logs off their session.

“Time Warp” application – Services leveraged in an AWS Region

The following diagram outlines AWS services leveraged by the “Time Warp” application within an “AWS Region” :

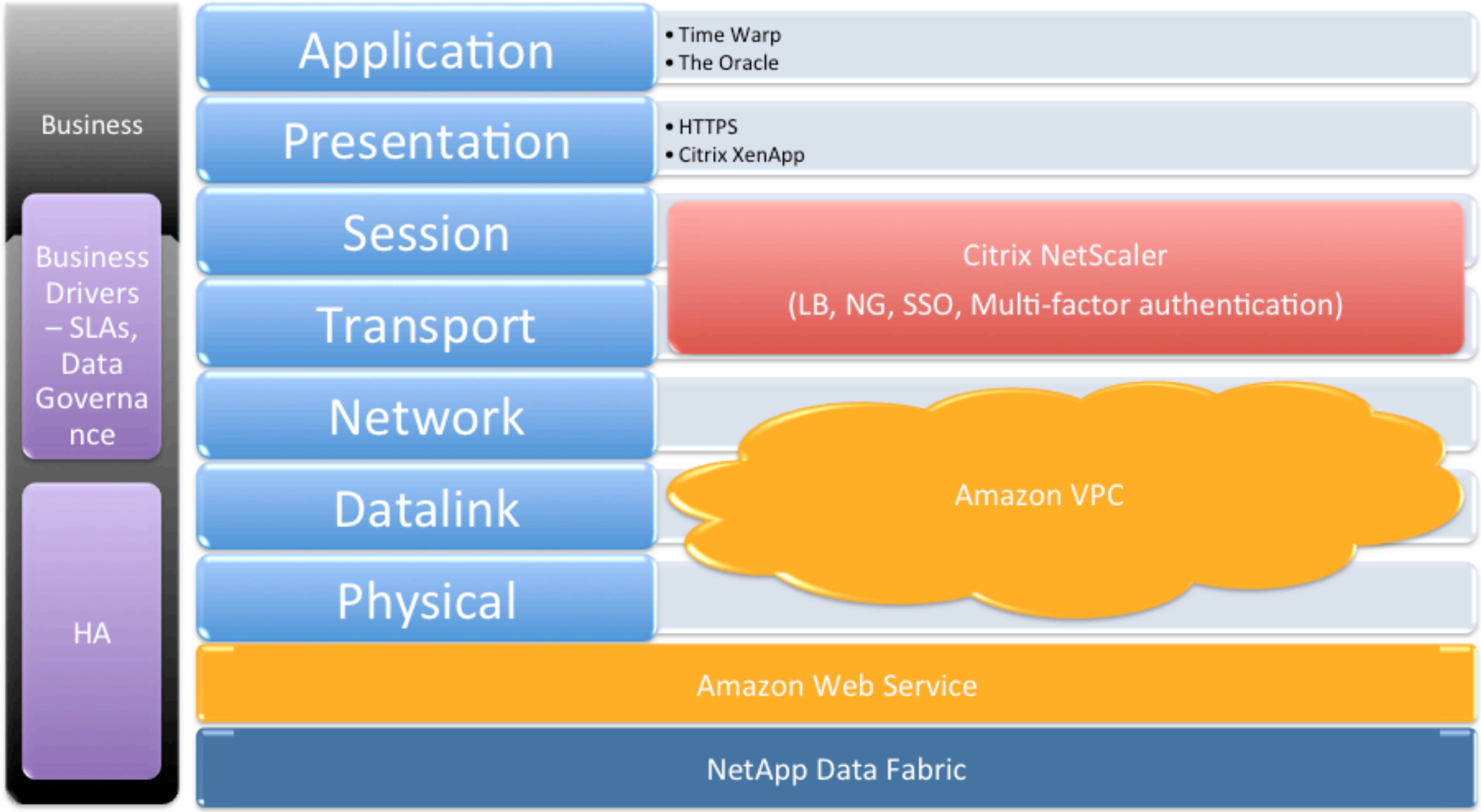


- Amazon Route53 DNS delegation to be used by Citrix NetScaler for Global Server Load Balancing Services.
- The Web Application, Caching and Database tier will have their dedicated subnets.
- Health of all services monitored using Amazon CloudWatch and custom scripts.
- High Availability of Enterprise Web Application provided by Citrix NetScaler Global Server Load Balancing services across availability zone within a region.
- Auto-scaling Web Application tier based on PHP based Linux instances. Amazon CloudWatch will be leveraged to monitor instance CPU and Memory utilization and will deploy new instances in the designated subnet, which will automatically get added to NetScaler load balancing algorithms.
- Scale-out Memcached cluster nodes spanning both Availability Zones in a Region to provide robust caching tier.

- Replication of MySQL database between the Availability Zones in a Region to provide High Availability in the database tier.

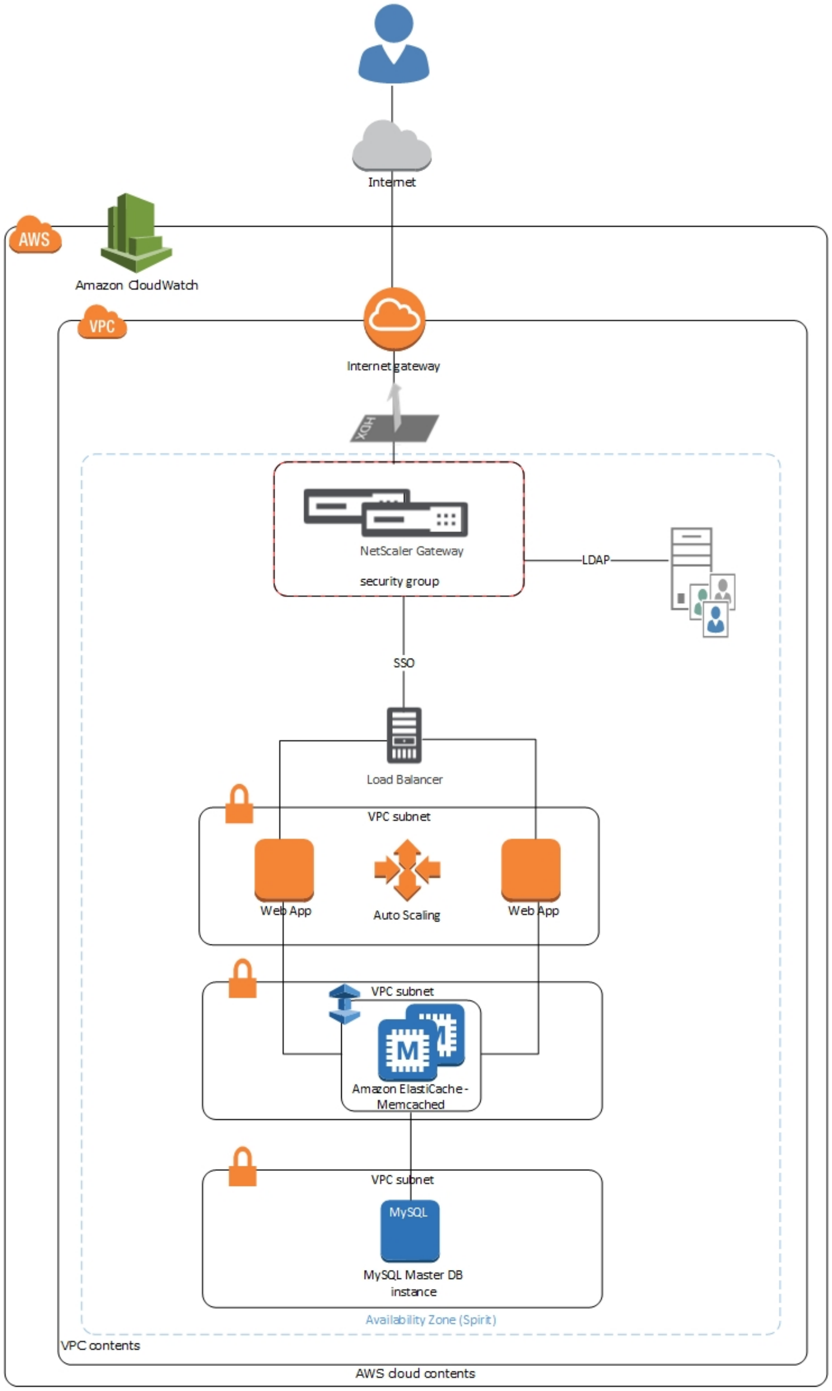
AWS Availability Zone Architecture

The following logical diagram outlines a single AWS Availability Zone, and the associated services provided within each layer of the technology stack:



“Time Warp” application - Services leveraged in an AWS Availability Zone

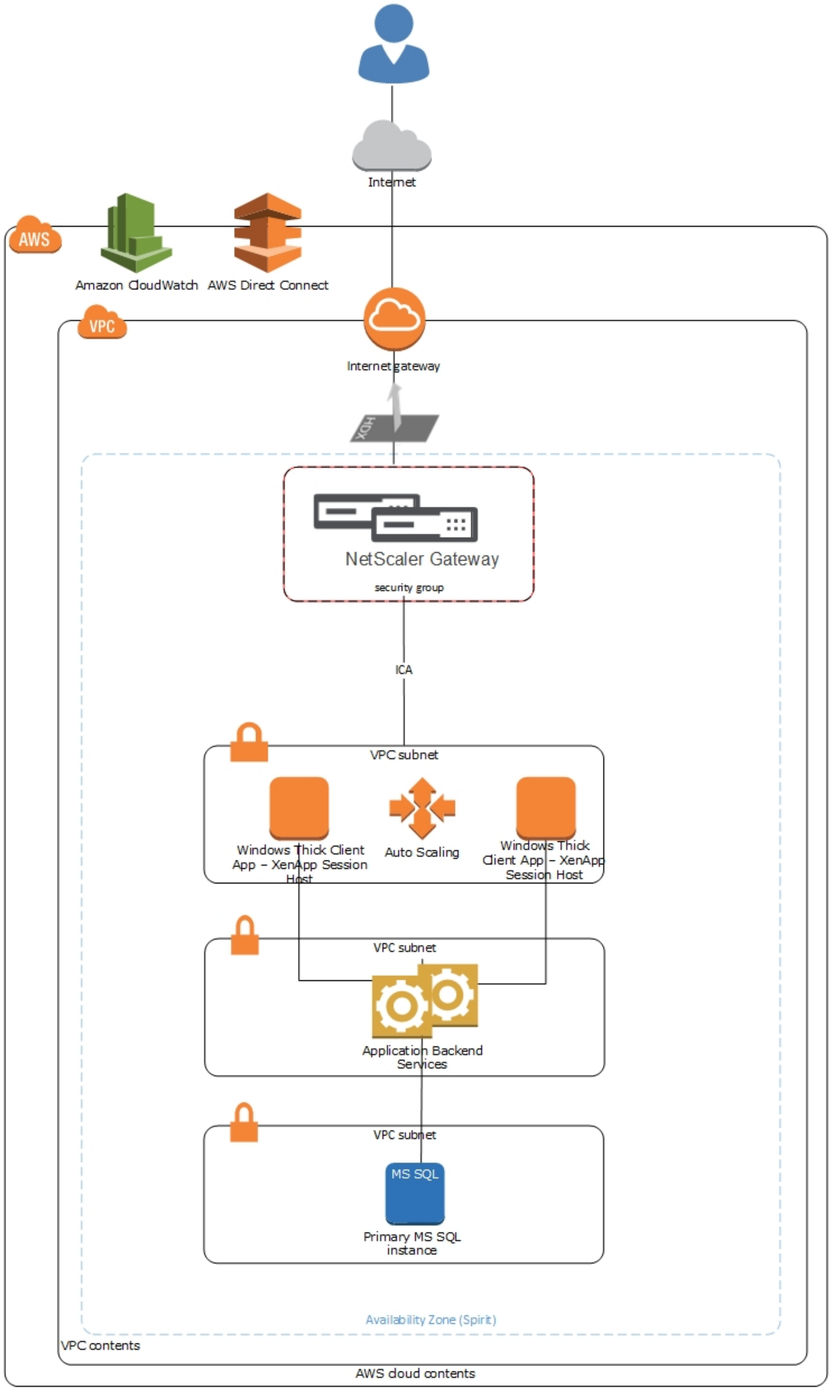
The following diagram outlines AWS services leveraged by the “Time Warp” application within an “AWS Availability Zone” :



- Citrix NetScaler Gateway provides Single Sign-On to Enterprise Web Apps and Windows applications.
- Citrix NetScaler will be leveraged for load balancing of the Web App to provide High Availability within each Availability Zone.

“The Oracle” application - Services leveraged in an AWS Availability Zone

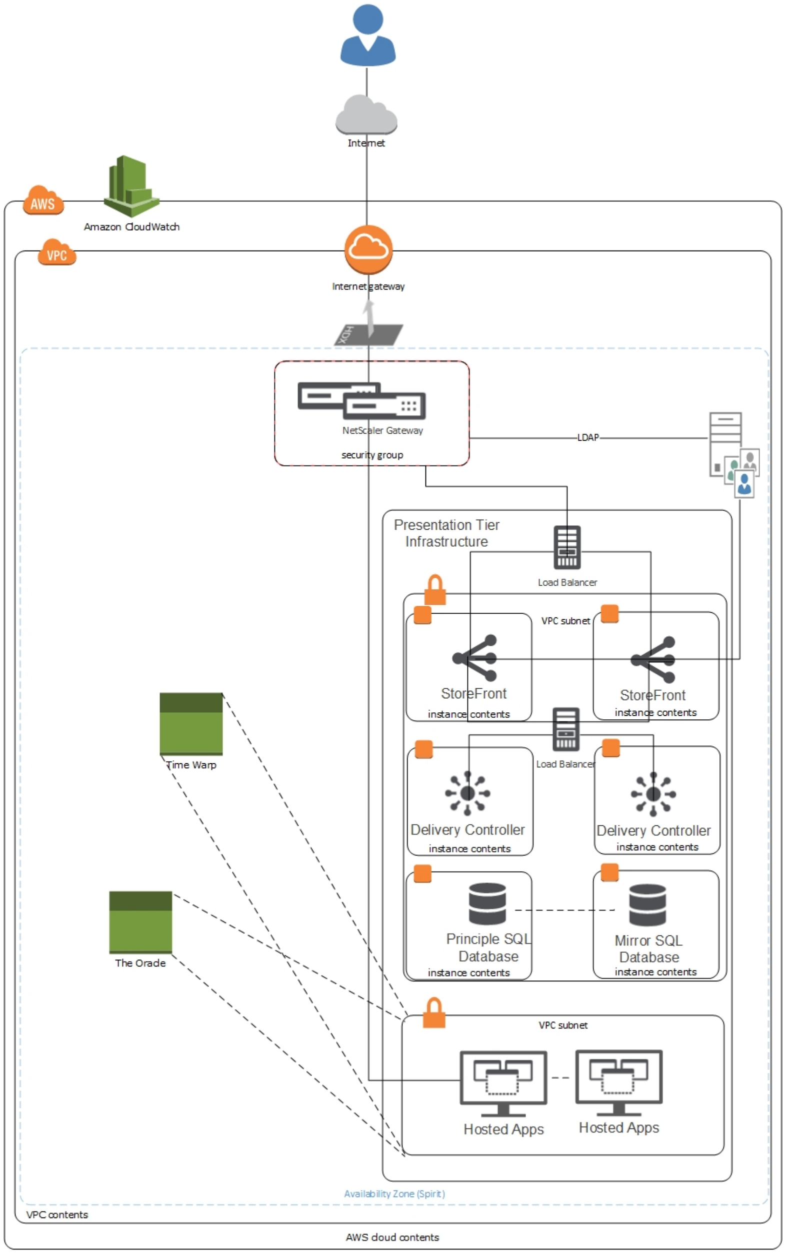
The following diagram outlines AWS services leveraged by the “The Oracle” application within an “AWS Availability Zone” :



- Citrix NetScaler leveraged for secure remote access to enterprise web apps and windows apps using Multi-Factor authentication.

Presentation Layer Infrastructure Components - Services leveraged in an AWS Availability Zone

The following diagram outlines AWS services leveraged by the Citrix Presentation Tier infrastructure components within an “AWS Availability Zone” :

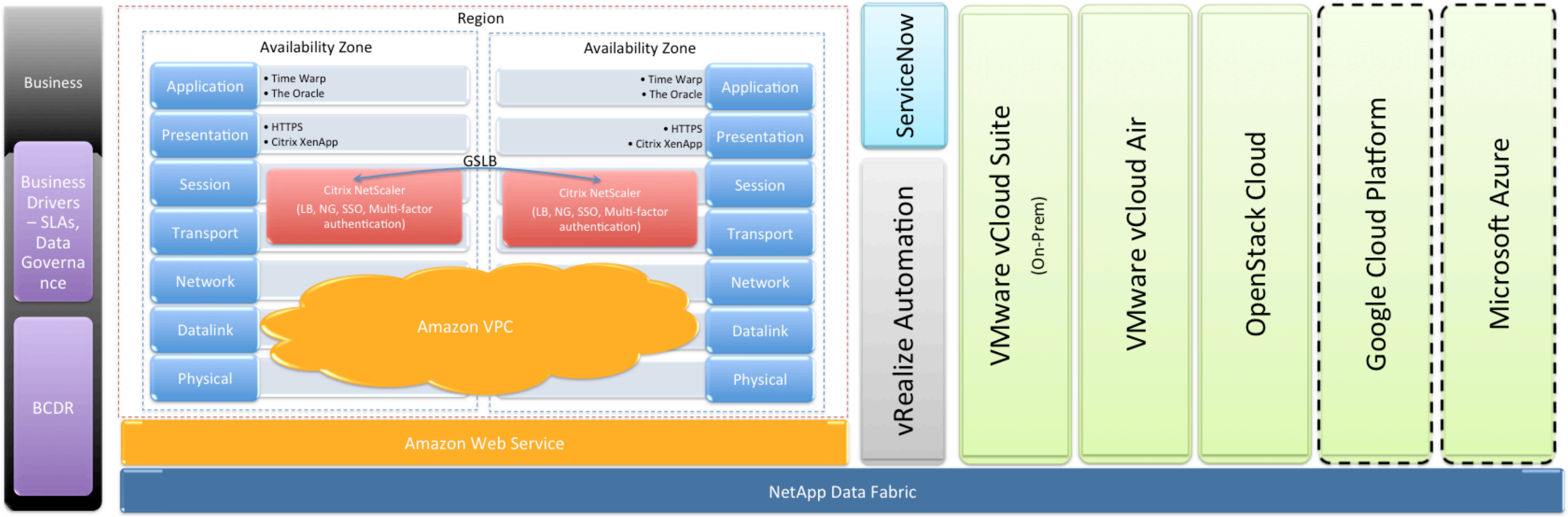


- Citrix NetScaler leveraged for secure remote access to enterprise web apps and windows apps.
- HA pair of Netscaler VPX Virtual Appliances leveraged in each Availability Zone.
- Robust and intelligent load balancing of HA pair of Citrix StoreFront provided by Citrix NetScaler.
- Robust and intelligent load balancing of HA pair of Citrix Delivery Controllers provided by Citrix NetScaler.
- Auto-scaling pool of Citrix XenApp Terminal Servers, leveraging AWS CloudWatch.

- Secure Remote Access to Enterprise Web Apps and Windows applications on any device.

“Phase 2” and future vision

The following logical diagram outlines “Phase 2” of the design and future vision :



- vRealize Automation will be leveraged as the cloud automation and orchestration framework of choice, as part of “Phase 2” and future vision of the Mars infrastructure.
- Hybrid cloud strategy to meet different application and data needs, such as Compliance, Data Sovereignty etc.
- Automation and orchestration framework that is cloud-agnostic and integrated with major public and private cloud solutions.
- Integration with industry leading IT Operations Management Software – ServiceNow.