Student Name: Tevin Achong
Student ID: 816000026
Course Code: INFO3606
Course Title: Cloud Computing
Assignment: 3

April 15, 2020

Question 1

The essential factors which an organization should be aware of before migrating to a cloud computing platform are:

- Business motivations, such as:
  - Capital and operational costs
  - Time-to-market
  - Mobility options
- Technical Motivations, such as:
  - Maintenance
  - Scale-up and scale-out facility
  - Application development and modernization
- Security and Privacy Motivations and Policies, such as:
  - How trustworthy the cloud service provider is
  - Being aware that the enterprise's data will be geographically located across different locations and each location or country may have its own privacy laws and regulations.
  - All the fundamental security mechanisms provided by the CSR: service availability; reliability; authentication; authorization; access control; confidentiality; integrity; auditing.

Question 2

As a cloud architect, I would deem that cloud migration is **not necessary** for this organization. The primary reason for this decision is the fact that *applications that experience unpredictable loads will benefit from migration, whereas applications that experience predictable or consistent loads are* ***best handled by the enterprise itself.*** From the problem description, the organization seems to experience consistent loads every half an hour or so. This means that it may best be managed in-house.

Some use cases in which cloud migration could be immensely useful include:

- applications experiencing huge traffic
- applications experiencing uncertain loads
- applications that need quick and continuous development and deployment
- applications that have growing storage demands
- applications experiencing peak loads as a result of seasonal traffic.

Based on the information provided, the oil and gas organization in question does not fall under any of the aforementioned categories.
Additionally, from a secuirty and privacy perspective, on migration data are naturally locked in with a provider and enterprises have no idea where their data reside. This is known as the data lock-in problem, and may be an issue for this organization if they ever wish to switch cloud service providers or leave the cloud entirely. Their main purpose for cloud migration would be to help them manage and transfer their data, so this needs to be taken into the most careful consideration. Furthermore, data stored in the cloud may suffer from the data remanence issue, which means that data may still be present (but flagged for deletion) in physical storage even after being deleted. If the data being transferred is sensitive, cloud migration would likely be a bad idea.

Question 3

Cloud service providers typically perform two major kinds of monitoring:

- Physical Monitoring
- Virtual Monitoring

Physical Monitoring

- Physical monitoring involves monitoring the physical infrastructure of the cloud. It deals with the internal status of cloud resources.
- From the cloud point of view it refers to the server level.
- Physical system monitoring is the basis for cloud system management as it is related to the physical computing infrastructure on which the cloud itself is built.
- It is here that conventional monitoring techniques such as computation-based tests and network-based tests are carried out.
- Computation-based tests are based on classical statistical measures such as mean, median, mode and temporal characteristics.
- Metrics measured by computation-based tests include: CPU utilization; CPU latency; CPU speed; CPU-related errors; memory utilization; memory page exchanges per second; memory latency; memory-related errors; and operating system metrics like system load;
- Metrics measured by network-based tests include: network latency; network utilization; network traffic; load patterns; network capacity bandwith; throughput; response time; round trip delay; jitter; packet/data loss; available bandwith; capacity, and; traffic volume

Virtual Monitoring

- Virtual system monitoring provides information about the virtual system characteristics of cloud services:
  - In IaaS cloud the system manager can monitor the status of every VM instance in the cloud and its internal resources.
  - In PaaS cloud the system managar can monitor the use of platform resources such as hosting space used and simultaneous network connections.
  - In SaaS cloud the system manager can mointor application usage patterns, resources shared among applications, etc.
  - Virtual monitoring is the main means of controlling quality of service metrics and ensuring service delivery according to the values mentioned in SLAs.
- Service providers use the metrics obtained from virtual system monitoring to calculate service costs and billing.
- Successful cloud business models almost always stem from virtual monitoring.

- Cloud users perform high-level monitoring determine how many resources they have consumed so that they can check their bills.
- In addition, such high-level monitoring makes it easy for consumers to compare the pricing of different cloud service providers.

Purpose of Monitoring the Cloud:

- Since there are physical and virtual resources that are distributed at different geographical locations in the cloud, without proper monitoring of cloud resources and services enterprises may fail to achieve the performance they set for themselves and benefits provided by the cloud.
- They run the risk of failing to achieve the return on investment targeted.
- Cloud monitoring is the process of monitoring, evaluating, and managing cloud-based services, applications, and infrastructure.
- Aditionally, cloud monitoring is fundamental to:
  - capacity planning
  - calculating the usage of resources and providing billing to consumers
  - identifying and addressing potential issues and providing troubleshooting
  - delivering services according to the service level agreement
  - providing detailed reports, in-depth graphs, and different metrics for performance management
  - optimizing cloud solutions and services
  - determining the status of resources hosted in the cloud
  - adopting control activities and performing various core activities of the cloud such as resource allocation
  - migrating without data loss
  - managing security
  - achieving those characteristics that are unique to the cloud: scalability, elasticity, and resource provisioning

Question 4

Six (6) core functions of Cloud Management Platforms (CMPs):

1. Service Request Management

    - This is a self-service interface provided by CMPs through which various cloud services are easily consumed by consumers.
    - Cloud services providers offer service catalogs with SLAs and cost details.
    - Based on the published information the CMP chooses the appropriate provider and services.
    - Service requests can be routed through this interface to the CMP solution to automate most activities.
    - Some users expect a service interface that serves as a pass-through to native capabilities within a public cloud service.
    - The service portal or marketplace is continuously updated with fresh features, functionalities, and facilities to gain an edge or retain the edge gained.
    - There are service and support management systems and other automation tools that readily fulfill varying requests from users.
    - There are operational team members employed by cloud service providers or third-party teams that team up together to fulfill service requests quickly.

2. Provisioning, Orchestration, and Automation

    - Provisioning, orchestration, and automation are the core capabilities of any CMP product.
    - There is an arsenal of tools intrinsically enabling these vital features. There are plenty of cloud orchestration, provisioning, and configuring tools that are made available these days.
    - There are industry strength standards for service and cloud infrastructure orchestration. Similarly, there are automation tools for job/task scheduling, load balancing, auto-scaling, resource allocation, etc.
    - There are resource configuration management systems. Software deployment and delivery tools are also hitting the market.
    - In a nutshell, cloud operations are being meticulously automated in an end-to-end fashion.

3. Monitoring and Metering

    - Monitoring, measurement, management, and metering are the basic requirements of any IT hardware and software packages.
    - Service usage and resource consumption need to be accurately measured and metered. There are a bunch of tools for accomplishing these.

4. Multi-Cloud Brokering

   - Brokerage solutions and services are very important at a time dominated by connected and federated clouds.
   - Interconnectivity, intermediation, and other enrichment and enablement capabilities are being performed through cloud service brokers.
   - There are connectors, adapters, drivers, and other solutions that establish a seamless linkage between public and private clouds.
   - There are bridge solutions to establish direct connectivity between public clouds.
   - Thus as a result of multiple clouds and services with different SLAs the role and responsibility of cloud brokers are bound to increase in the days ahead. Advanced CMPs are being fitted with brokerage tools and engines.

5. Security and Identity

   - Concern over security is widespread among cloud users who rightly insist on security requirements in the cloud environment.
   - As customer-facing applications and data (corporate, customer, and confidential) are being held in the cloud environment, especially in public cloud, security is paramount. User identification, authentication, authorization, and other accountability and auditability are being pronounced as the most critical and crucial for continued spread of the cloud.
   - The security and privacy of data while in transit, persistence, and usage are paramount for the intended success of the cloud idea.
   - Key-based encryption and decryption, key management, etc. are getting a lot of attention these days. Single sign-on (SSO) is indispensable to multi-cloud applications.
   - United threat and vulnerability management solutions are becoming highly popular in the cloud environment.

6. Service-Level Management

   - Ensuring service-level and operation-level contracts agreed between cloud consumer and server are complied with is an important facet of the cloud arena.
   - Non-functional requirements (NFRs)/quality of service (QoS) attributes stand out as the key differentiators among all participating service providers.
   - Scalability, availability, fault tolerance, security, and dependability are often repeated needs.
   - Service resilience, application readability, and infrastructure versatility are given utmost importance for boosting user confidence in the cloud "mystery".
   - There is a stunning array of toolsets that can be used to facilitate these complex capabilities.

Question 5

Five (5) reasons why Cloud Service Brokerages (CSBs) are needed:

1. Cloud service brokerages help organizations select the best cloud services for that organization's needs.

2. Cloud service brokerages support line-of-business requirements, and meet IT demands across disparate cloud without jeopradizing performance or security.

3. Cloud service brokerages may assist in the deployment and integration of applications across multiple clouds.

4. Cloud service brokerages may provide options and possible cost savings by providing a catalog that compares competing services.

5. Cloud service brokerages are master orchestrators who can manage the complexity of multiple cloud ecosystems and transform businesses into digital enterprises.

Cloud service brokerage serves as an intermediary between cloud providers and cloud consumers. It assists companies in choosing services and offerings that best suit their needs. Cloud technology is increasingly playing a major part in bringing about digital business. The rapid adoption of cloud services from multiple cloud service providers (CSPs) and communication service providers creates a unique set of challenges for IT, specifically because enterprise IT teams must now orchestrate onboarding, managing, and delivering IT and business services from multiple portals and vendors. Such multiplicity makes it tough to ensure consistent performance, security, and control within the multi-cloud ecosystem and is the reason cloud brokerage platform solutions are becoming popular.

Question 6

Cloud Orchestration

- Orchestration is concerned with automating multiple tasks together. Processes typically comprise multiple tasks and systems.
- The tasks inscribed in a process need to be executed in sequence to be fruitful.
- That is, a process starts with an appropriate workflow representation and end with workflow execution.
- Thus a process from workflow representation to workflow execution is simply termed orchestration.
- Orchestration deals with the end-to-end process, including management of all related services, taking care of high availability (HA), post-deployment, failure recovery, scaling and more.
- Automating tasks or orchestration of workflows within a single enterprise may be easier as all the services, such as APIs, interfaces, standards, regulations, and policies, are confined within the enterprise.
- However, enterprises now find themselves compelled to look at cloud offerings to meet many critical needs such as reduced capital and operational cost, uncertain loads, dynamic and unlimited scalability needs, and high availability. They depend on public clouds because of their inherent capabilities. At the same time enterprises have to depend on on-premises setups to protect legacy and sensitive data.
- In spite of the challenges associated with a multi-cloud environment, enterprises are compelled to opt for multi-cloud and hybrid IT because of their benefits.
- Cloud orchestration resolves some of the challenges associated with operations in multi-cloud environment.

Four (4) functions of the Orchestration Engine:

1. helps automate delivery of infrastructure, application, and custom IT services
2. supports direct integration of service management capabilities
3. deploys application workloads across on-premises and off-premises environments
4. provides policy-based governance and logical application modeling to help ensure that multi-vendor and multi-cloud services are delivered at the right size and service level for each task performed.