UNIVERSITY OF ALBERTA

HYBRID CLOUD ARCHITECTURE
DESIGN, DEPLOYMENT AND ANALYSIS

Submitted by:
Kristoffer Angelo Soliven

A MINT 709 Capstone Project submitted to the Departments of Computing Science and Electrical and Computer Engineering of the University of Alberta in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN
INTERNETWORKING

Edmonton, Alberta
Convocation: June 2020

[This page is left intentionally blank]

Table of Contents

List of Tables

List of Figures

[This page is left intentionally blank]

Section 1: Introduction

Overview

Since 2016 and based on thousands of surveys and forecasts performed by Gartner, one of the world's leading research and advisory company, its has become evident that cloud computing is now a key component within most organizations' IT strategies. This is evident due to the number of current software vendor and service provider organizations that offer their solutions through Cloud-based strategies. (Hanyes, 2018)

This now raises the question: "What will now happen to traditional and on-premise corporate IT environments?"

While traditional/on-premise solutions have their advantages, these are being overlooked due to the flexibility, scalability, cost-effectivity, and on-demand requirements of modern-day businesses, which are all being provided by Cloud-based technologies. Due to these factors, most traditional/on-premise business solutions are migrating to these external cloud services.

However, there are still various factors, primarily the business requirements, that would drive organizations to select traditional/on-premise solutions over Cloud-based strategies. Legacy technologies that are not supported by any Cloud-based technologies would still force the utilization of conventional/on-premise solutions for their business needs. Legal requirements could also draw limitations for organizations to utilize Cloud-based solutions within their organization. These various factors would affect the decision and implementation of IT strategies within organizations. Thus, bringing together the best features from both traditional and Cloud-based technologies to solve a business requirement(s) must be realized to maximize resource usage, cost-efficacy, and optimize business operations.

Purpose

This paper focuses on the design, deployment, and analysis of Hybrid Cloud Architectures. This paper will be discussing general and generic traditional and on-premise solutions and three (3) of the primary cloud service provider in today's market namely Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) and some select services related to compute, networking, storage, database, management, monitoring, security, and migration.

Scope

The paper will be looking into the design best practices, analysis of these cloud resources, deployment, and migration schemes. It will be focusing on the following areas:

- Business Requirements
- Capital and Costs
- Legal Compliance
- Setup and Management
- Engineering Time
- Licensing
- Data Availability (HA)
- Disaster Recovery (DR)
- Security

Objective

Planning a Cloud Architecture to solve a specific business problem does take a considerable amount of time. It determines how effective the implementation(s) will be able to perform the business requirements and deliver its desired outcomes. There is indeed a need to create a framework to provide business enterprises with smarter decisions optimized to solve its business-related requirements.

The paper aims:

- To create a documentation that will provide an understanding of the Cloud Architecture, its components, platform implementations, and planning considerations
- To establish a comparison between all Cloud Architectures being implemented on enterprise networks namely the Private, Public and Hybrid Cloud Architectures
- To provide the business management with a design and deployment framework that can be used to set standards on making appropriate decisions to optimize business operations while minimizing costs
- To deliver business scenarios with unique business requirements and analyze the specific solutions that will be utilized based on several factors, namely:
    - Business Requirements
    - Capital and Costs
    - Legal Compliance
    - Setup and Management
    - Engineering Time
    - Licensing
    - Data Availability (HA)
    - Disaster Recovery (DR)
    - Security
- To establish Cloud systems that will be using Public Cloud platforms such as AWS, Azure, and GCP in combination with Private Cloud solutions to create a Hybrid Cloud Solution to solve a business requirement.

Section 2: Cloud – Evolution, Concepts, and Architecture

Evolution of Cloud

Cloud computing is one of the major actors that leads to the next generation of the Internet and Virtualization. It provides optimized and efficient computing through enhanced collaboration, agility, scalability, and availability. It also delivers a platform for local and remote computing, which reduces capital hardware- and software-related costs and minimizes physical footprint within an organization. (Bojanova & Samba, 2011)

The development of connectivity on the Cloud did undergo several phases and can be summarized into a five (5) evolution stages:

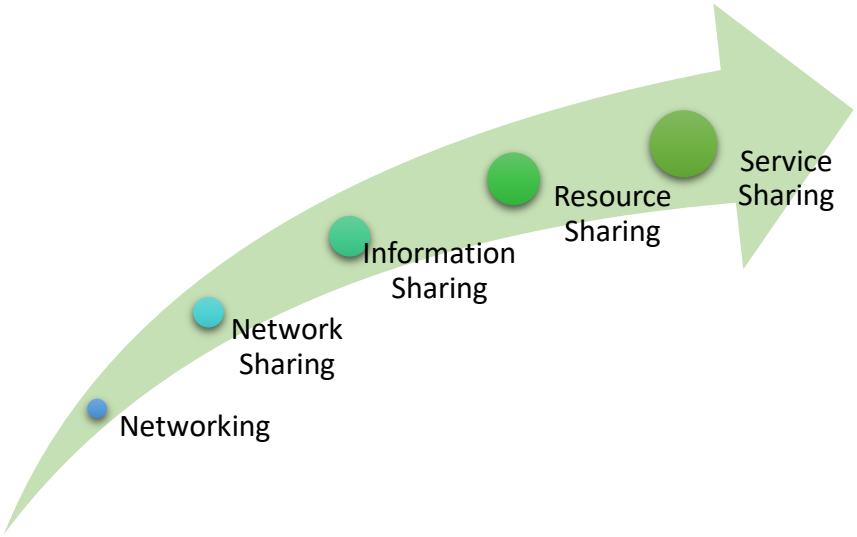

Figure 1 - Evolution of Cloud

First Stage – Networking

In this stage, the TCP/IP abstraction was created. Multiple end-devices have been connected to networks meant for private institutions such as universities and national laboratories.

Second Stage – Network Sharing

These various private networks from the First Stage have been connected to share resources with one another. It is the interconnection of networks, which leads to the emergence of the Internet.

Third Stage – Information Sharing

The next stage, which focuses on data transfer, was the World Wide Web (WWW) data abstraction. This led to the exchange of information between users through the Internet via Hypertext Transfer Protocol (HTTP) displayed using Hypertext Markup Language (HTML).

Fourth Stage – Resource Sharing

The fourth stage then emerged with the creation of standards to focus on local and remote resource sharing and collaboration. This is characterized by the Virtualization and Cloud Computing technologies.

For the first three (3) stages, all stages have been using dedicated devices such as servers to process specific tasks. However, this setup wastes a lot of power, underutilizes its compute capabilities, and has a single point of failure. With these limitations, Virtualization was developed to share resources between applications and physical end-devices processing these applications. (Cisco NetAcad, 2019)

Virtualization is defined as the separation of the operating system to the physical hardware. It is the foundation of Cloud computing. Cloud computing is defined as the separation of applications to physical hardware. Cloud computing is not possible without the development of Virtualization.

Fifth Stage – Service Sharing

The newest stage for Cloud Computing is service sharing, which provides an abstraction to simplify the infrastructure complexities of servers, applications, and networking platforms. Cloud Computing has created a delivery model for service providers to offer several computing services that consumers would need to satisfy their requirements and deliver solutions.

According to the U.S. Government's National Institute of Standards and Technology (NIST), Cloud Computing enabled a model "for convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or services provider interaction." (Grance & Mell, 2011)

Cloud Concepts

Virtualization vs. Cloud Computing

Virtualization

Virtualization is the separation of the operating system to the physical hardware. As it is the foundation for Cloud Computing, it is useful to discuss the abstraction of Computing Architecture to describe how Virtualization works. A computing system consists of the following abstraction layers:

Computing Architecture Abstraction Layers

i. Services – Applications and features provided by a computing device
ii. Operating System (OS) – It is the system software managing computing hardware and software resources.
iii. Firmware – It is a software providing low-level control for the device's hardware
iv. Hardware – It refers to the physical parts of a computing device which executes the software

An abstraction layer is then interfaced between the layers above and below it by some type of programming code (e.g., C and C++). (Cisco NetAcad, 2019)

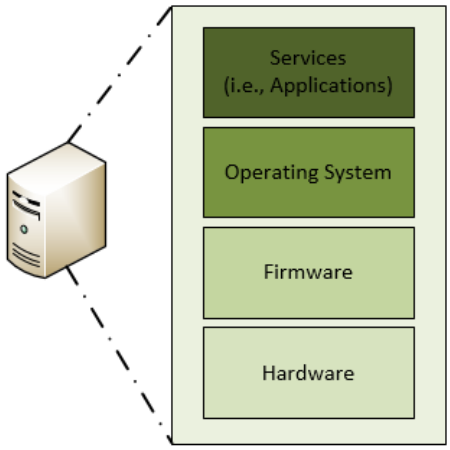

Figure 2 - Computing Architecture Layers

Virtualization is made possible with Hypervisors. Hypervisors (i.e., host machines) are hardware and software that enables Virtual Machines. Virtual Machines (i.e., guest machines) are individual instances of a computer system emulation which provides the same services as that of a physical computing device (e.g., Servers).

There are two (2) types of Hypervisors:

1. Type 2 Hypervisors – It is a "hosted" approach since that it is a software that runs with the OS and hardware of the device in which it is hosted and executed.

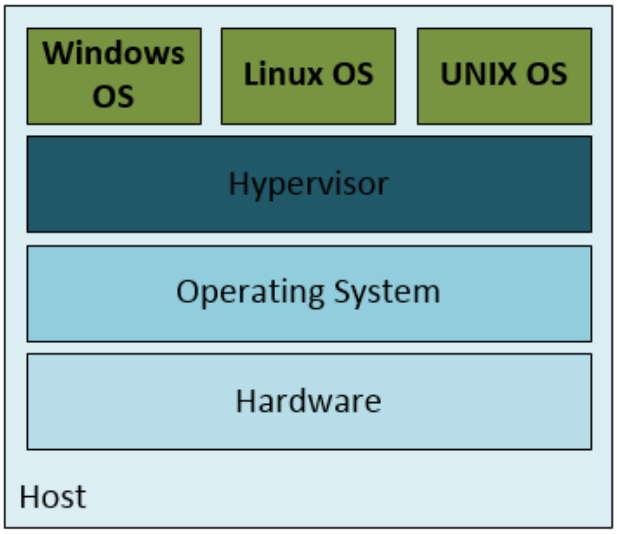

Figure 3 - Type 2 Hypervisor

Examples of these Type 2 Hypervisors includes the following:

- Virtual PC
- Mac OS X Parallels
- Oracle VM VirtualBox
- VMware Workstation
- VMware Fusion

2. Type 1 Hypervisors – It is a “bare-metal” approach since it is directly installed on the hardware. These Hypervisors are typically implemented by enterprise organizations and data center environments.

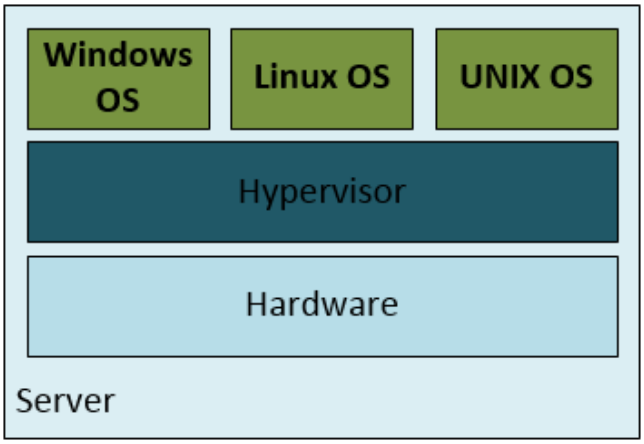

Figure 4 - Type 1 Hypervisor

Examples of these Type 1 Hypervisors includes the following:

- Xen
- VMware ESXi
- Oracle VM Server
- Microsoft Hyper-V
- Linux KVM (Kernel-based Virtual Machine)

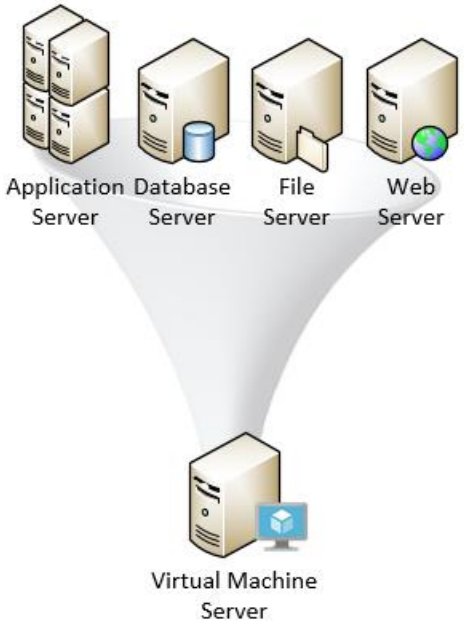

Figure 5 - A depiction of Virtualization

Cloud Computing

According to NIST, “Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources which can be provisioned rapidly and released with minimal management. (Grance & Mell, 2011)

Cloud Computing is the separation of applications to the physical hardware, which can be accessed either locally or remotely. It is not possible without the development of Virtualization.

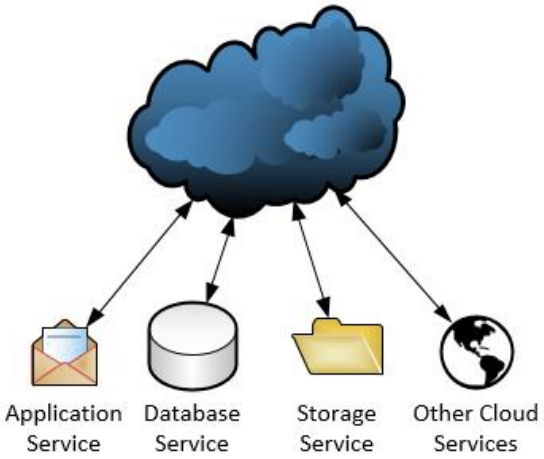

Figure 6 - A depiction of Cloud Computing

Data Center vs. Cloud

The terms data center, cloud, and cloud computing are often misused and do, sometimes, create confusion based on how it is used in a context. The following will provide appropriate descriptions to each of these concepts (Cisco NetAcad, 2019)

Data Center

Data Centers are typically data processing and storage facility managed by an on-premise IT department or leased/collocated offsite. A data center can occupy multiple rooms of a building, with one or more floors or even an entire building or set of buildings. It houses several computing systems and their associated resources and components. Data centers are costly to build, manage, and maintain. Because of this cost aspect, only most large organizations are using privately built data centers for their private use and to provide services to other users.

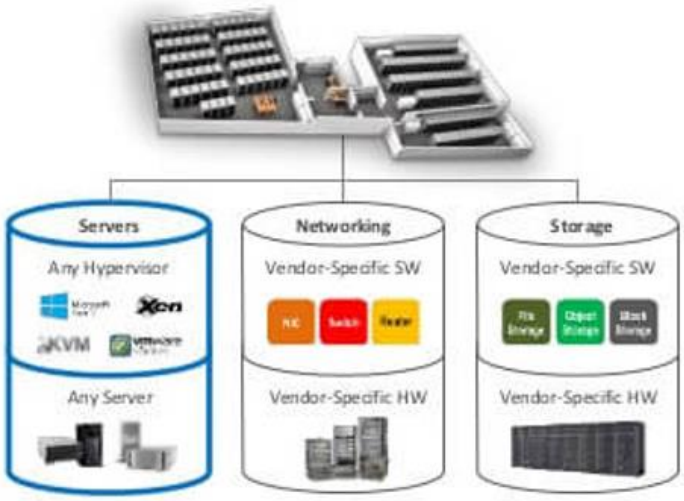

Figure 7 - Data Center Structure
(Jain, 2019)

Cloud

Cloud is an off-premise environment that offers on-demand access to a shared pool of configurable computing resources, which can be rapidly provided with minimal complexity and effort. Cloud and Cloud Computing is made possible with virtualization within data centers. Organizations that are unable to build their own data centers due to cost constraints can reduce this cost factor by availing services from larger organizations providing such services over the cloud.

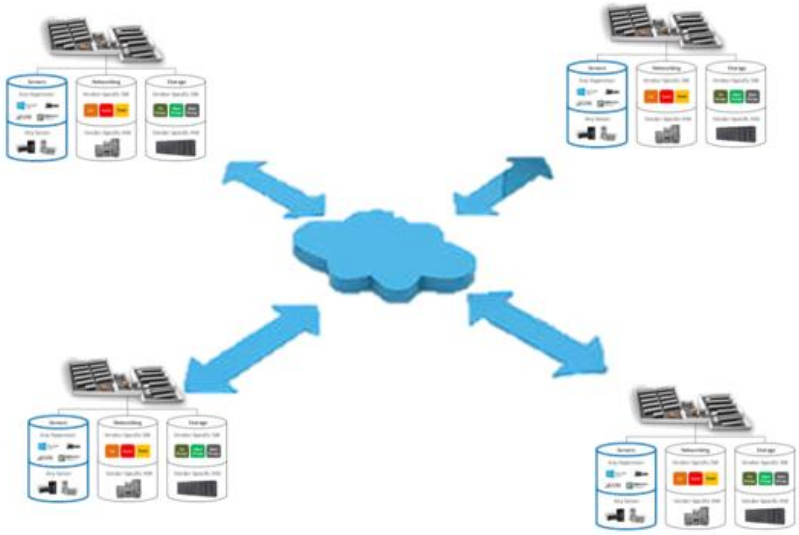

Figure 8 - Cloud Structure
(Jain, 2019)

Fog vs. Cloud

The concepts of both Fog and Cloud Computing are interconnected. As a metaphor, in nature, fog is closer to the earth's surface as that of the cloud. This is true in comparison to the world of computing technology, such that Fog is closer to end-devices compared with the Cloud. (Sakovich, 2018)

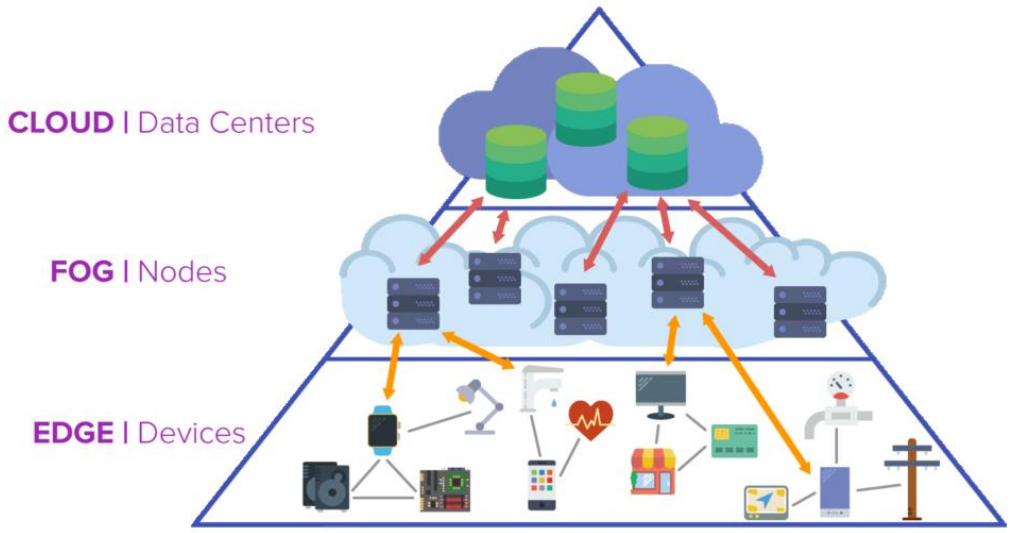

Figure 9 - Fog vs. Cloud Computing (ERPINNEWS, 2018)

Fog computing can be considered as an extension of Cloud computing and acts as an intermediary link between hardware and remote servers. It consists of multiple nodes/cloudlets which are physically closer to devices relative to data centers or clouds. (Sakovich, 2018)

Fog computing provides instant connections to end-devices, supports resource-intensive applications (e.g., IoT), and regulates information that can be processed locally or must be sent to distant data centers or cloud environments. This is an intelligent way to control the efficient use of resources within a computing system.

Cloud Actors

According to NIST, five major actors have been identified in cloud computing. The NIST Conceptual Reference Model diagram shows the actors who are discussed below. (Liu, et al., 2011)

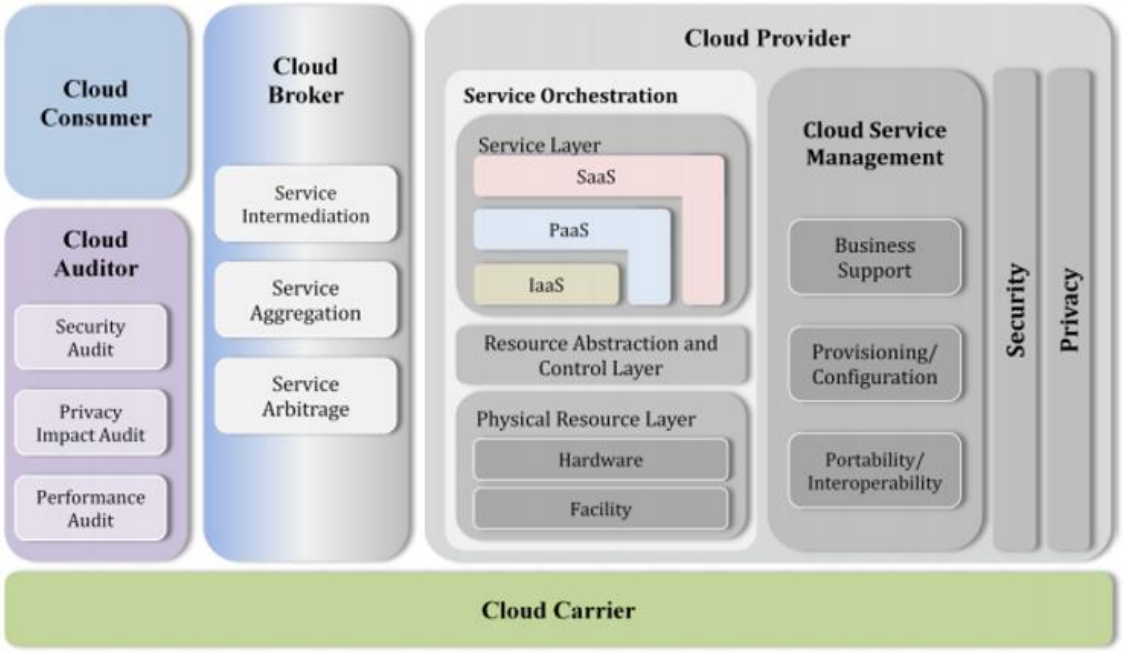

Figure 10 - Cloud Actors and Roles
(Liu, et al., 2011)

a. Cloud Consumer: A person or organization that utilizes services from Cloud Providers.
b. Cloud Provider: A person or organization that is responsible for providing services to interested consumer organizations.
c. Cloud Auditor: An entity that performs assessments to cloud services, operations, performance metrics, alignment to existing standards, security and implementation.
d. Cloud Broker: An entity that acts as an intermediary body between Cloud Consumers and Providers that serves as a useful tool to negotiate the terms, negotiation, and management of services to be availed from such providers.
e. Cloud Carrier: An entity that provides connectivity between these other Cloud Actors.

Cloud Computing

What is Cloud Computing?

As discussed from the previous sections, Cloud Computing is derived from the existence of Virtualization and Data Centers and is motivated due to its cost, availability, and flexibility.

To summarize its definition, Cloud computing is the separation of the application from the physical hardware made possible via Virtualization. It is an off-premise service that enables ease of access to globally available cloud services provided by these service providers. It facilitates on-demand network access to a shared pool of configurable computing resources (e.g., networks, compute, and storage), which can be provisioned with minimal complexity and effort.

Organizations that are unable to build their own data centers to deliver their business requirements due to constraints involving cost primarily resolves this with the utilization of cloud services available from various cloud service providers. Cloud Computing is now a delivery model for IT services that enhances collaboration, agility, flexibility, and availability of resources that aim to resolve specific requirements within an organization.

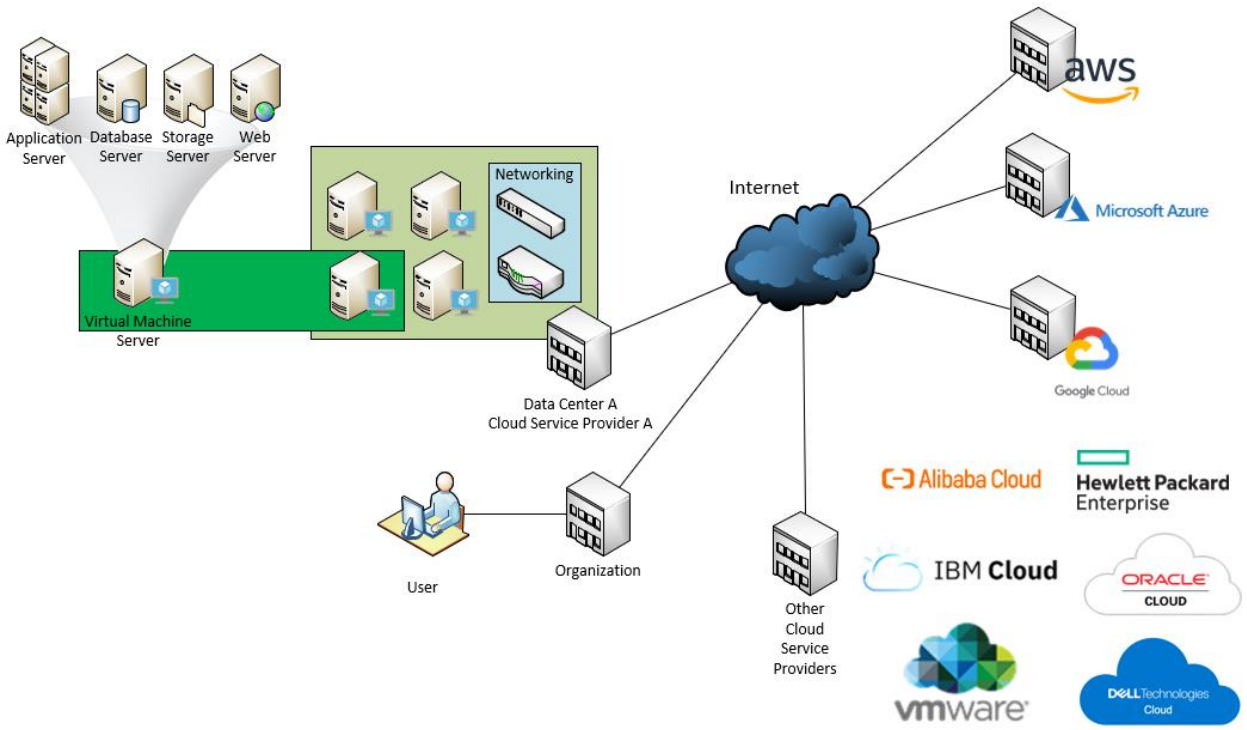

Figure 11 - A typical Cloud topology

The delivery of Cloud Computing is due to an effective computing architecture. Cloud Architecture refers to various resources required and engineered to solve business problems. It defines the technology that is used to solve such issues and the relationships existing between them. A computing system can be divided into two sections: The Front-end and the Back-end components.

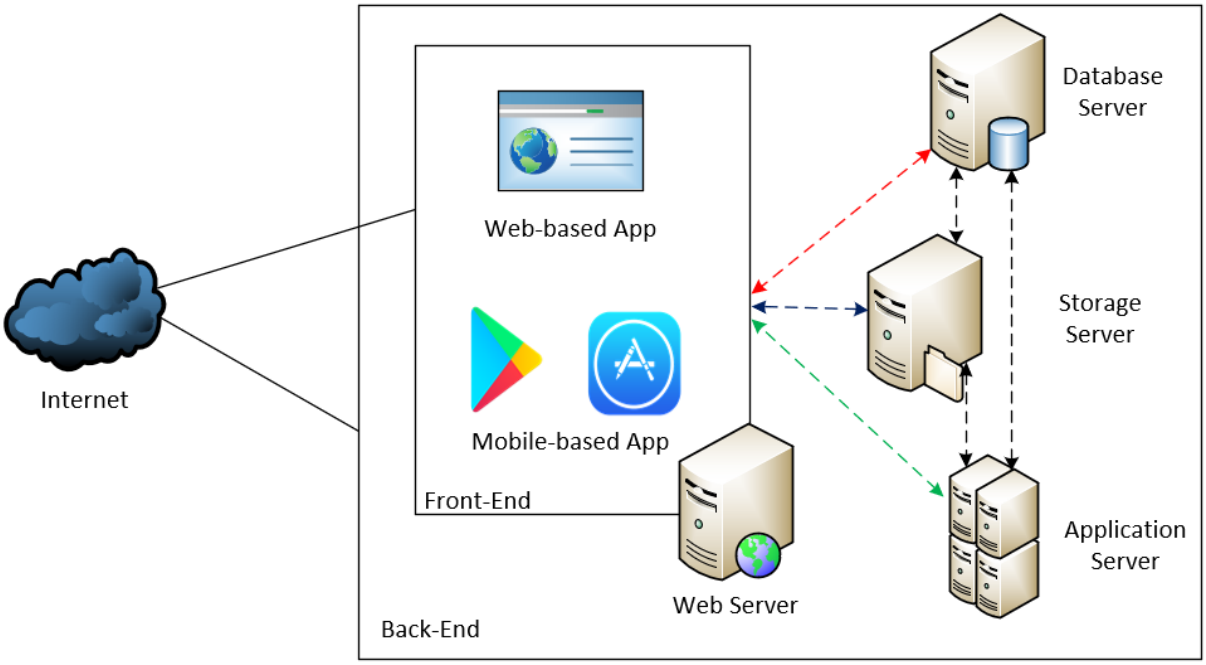

Figure 12 – Example Front-End and Back-End System Topology

The Front-end is what the end-user is interacting with, such as the computer (or the computer network) and the applications required to access different services offered by a cloud computing system. On the other hand, the Back-end, which includes various computing resources such as servers, compute instances, networking devices, storage, and its relationship with each other, makes up this "cloud" of computing services. (Strickland, 2008)

Front-End Systems

All elements which are closer to human interaction are part of the Front-end Systems. This could include user end-devices such as workstations, laptops, tablets, and mobile phones, together with the application in which is hosted and executed from one or more computing system locations (e.g., local network and cloud). Front-end systems are critical to interface the user and the computing system in order to perform the requested actions and produce the relevant outputs to be used by the end-user.

Back-End Systems

Back-end Systems perform and executes everything that is being processed in the Front-end Systems. In order for the Back-end System to support the operations of a particular system it was designed to operate with, considerations on these following areas must be made to properly organize and arrange the system infrastructure accordingly based on industry standards and best practices.

1. Physical Infrastructure
2. Server (i.e., Physical and Virtual Compute Resources)
3. Storage
4. Network
5. Management Policies

Several aspects of a Cloud Architecture must be considered on its design, but the following are critical in implementing a Cloud Infrastructure, namely Compute, Network, Storage, Database, and Security Resources. Compute resources are the technology used to perform process execution which includes computers, servers, virtual machines, and other devices that utilizes processor cores from a set of devices that can be executed on-premise or remotely on the cloud. Network resources are what establishes the relationship between on-premise and cloud devices to correctly transfer a message from a source to a destination device(s) and maintain the network connection between them. Storage and Database devices are essential in storing data used for business processes that can be located on-premise or on the cloud. Lastly, Security resources are devices and set of features that provide information security for all information being processed and transferred in the system. (Duffy, 2019; Kroonenburg, 2019)

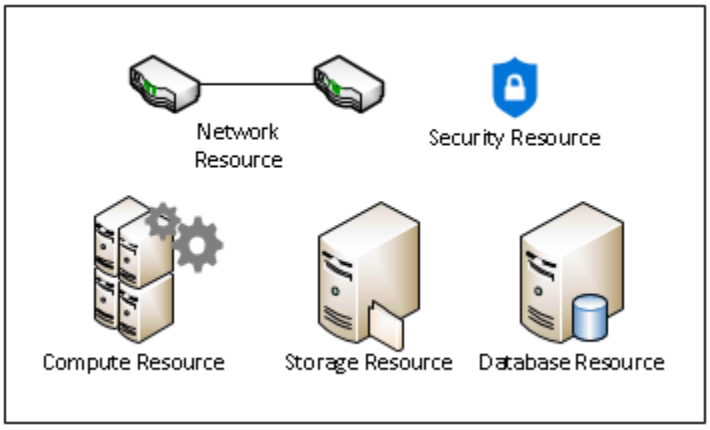

Figure 13 - Major Cloud Architecture Resources

There are three (3) major types of storage formats, namely File, Block, and Object Storage. File Storage, also known as File-level or File-based storage, is a storage format that utilizes folders and paths to provide data hierarchy and proper organization. This is usually seen in systems that utilize folders such as with Windows Explorer. The drawback, however, with this system is that it must scale-out (i.e., to increase by adding a new storage capacity) in order to upgrade the system capacity rather than scale-up (i.e., to increase by upgrading the storage capacity). Block Storage is a storage format, generally seen on Storage Area Networks (SAN), that divides data into arbitrarily sized blocks which allow such information to be stored wherever is most convenient. Once the data is re-accessed, the underlying software then reassembles that data for use. As a disadvantage, implementing a block storage system is costly and has a limited ability to handle metadata which could be an issue if implemented with an application or database service(s). Lastly, Object Storage is a storage format that uses metadata to relate all fragmented data stored in the system. Utilizing this type of system requires API integration services and is well suited for storing static data in the public cloud. However, manipulating information in the Object Storage limits any modification within files and writes a file(s) completely at a time (Red Hat, 2020). In summary, File Storage is best used for regular local enterprise file and storage services, Block Storage is best used for SAN purposes, and Object Storage is best used for unstructured and static data that will be written once and read multiple times since it primarily uses APIs and metadata to handle data queries. There are some new and improved features, however, that aim to combine all the benefits between these types of solutions which will not be covered in this documentation.

In order to save storage space, optimizing the data stored within these solutions must be considered. This is done by Data Deduplication, which is a technique used to enhance the efficiency of the storage environment's utilization by removing duplicate copies of raw data.

There are two major types of data deduplication, namely File-level Deduplication and Block-level Deduplication. File-level deduplication, also known as Single-Instance Storage (SIS), is an indexed based approach such that any files that will be stored in a storage system will be compared with all other data stored within the system. If it is unique, the data is stored together with its updated index and if not, it will only store a pointer to an existing file. This scheme effectively minimizes the use of storage space through the use of these indexes. On the other hand, Block-level deduplication is similar in concept with File-level deduplication with the use of indexes. However, instead of assigning an index to a file, discrete chunks of data stored within this Block Storage is assigned by a unique index identifier such that when new data blocks are stored, it will be added accordingly and if a data block is already existing into the storage environment, only a pointer is stored to this data block. (Whitehouse, 2008)

There are two Database solutions available that are used to perform processes through applications. These are the SQL and NoSQL. SQL (Structured Query Language) is a relational database that uses a rigid way of storing information through tables/entities/collection, columns/fields, and rows/records. It uses schemas due to its predictable and structured data sets, relations to easily provide association and aids with easier data modification. The drawback, however, is that it is not flexible with data, restrictions exist with completing complex queries (e.g., read requests of multiple records) and is mostly limited with vertical scaling (i.e., scaling-up). NoSQL (No SQL) is a non-relational database that is flexible on how it stores information as it is schema-less. It has no or few relations within its data set, which is great for read queries as it combines unrelated information into a collection, and horizontal (i.e., scaling-out) and vertical scaling (i.e., scaling-up) is possible. The drawback for this type of database is that as this is schema-less, information within a record is unreliable as it does not contain some specific information based on the requested query and there is also a limitation with completing complex queries (e.g., write requests that would modify multiple collections of information) (Academind, 2018). To summarize, SQL is best used for structured datasets, and complex write requests from related data collections, while NoSQL is best used for unstructured datasets and complex read requests from unrelated data collections. There are some new and improved features, however, that aim to combine all the benefits between these types of solutions which will not be covered in this documentation.

In general, Cloud Computing is composed of five essential characteristics, three service models, and four deployment models.

Cloud Computing Characteristics

NIST provides five characteristics of the cloud and is as follows: (Grance & Mell, 2011)

a) On-demand self–service: A person or organization can instantly provision computing capabilities (e.g., compute, storage, and network) on an on-demand basis. These are allocated automatically without human interference.
b) Broad Network Access: End-users can access the network together with its cloud services across thick or thin client devices (e.g., workstations, laptops, tablets, and mobile phones) through standard mechanisms.
c) Resource pooling: The provider’s pool of resources is established to support multiple consumer clients or tenants. This multitenancy enables the sharing of these pooled resources and can be customized to satisfy an organization’s business requirement(s).
d) Rapid Elasticity: Capabilities and resources offered by cloud service providers can be rapidly deployed, scaled, and released. These services must be able to seamlessly scale-up/down such that it appears that the providers' capabilities are unlimited for consumers.
e) Measured Service: Cloud systems automatically monitor and control some aspects of the service being provided to clients (e.g., storage, compute, and bandwidth). This resource usage is then presented to both the cloud consumer and provider, enabling transparency to both entities.

Cloud Service Models

Cloud services are available in several options designed to deliver customer requirements. The three main cloud computing services defined by NIST are as follows:

Software-as-a-Service (SaaS)

For this service model, the cloud provider is responsible for delivering services (e.g., Office 365 and custom software applications) over the Internet. (Cisco NetAcad, 2019)

Providers offer a hosted set of software solutions running on an infrastructure that is designed and developed to be accessed simultaneously by multiple cloud consumers over the Internet. These software applications are all managed by these providers and ensure that the systems are secured, available, and up-to-date. Some SaaS providers host these applications from other cloud providers' PaaS or IaaS offerings. (Odun-Ayo, Ananya, Agono, & Goddy-Worlu, 2018)

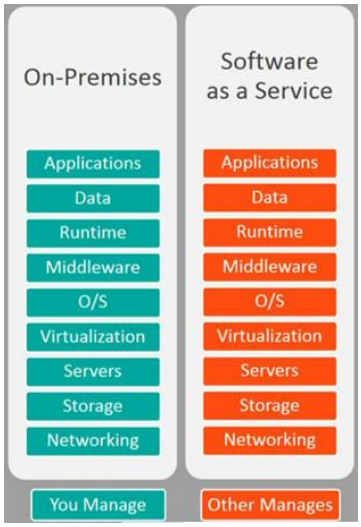

Figure 14 – Software-as-a-Service (SaaS) (Watts & Raza, 2019)

Examples of SaaS:

i. Email and Office Productivity:
   - Email applications, word editors and processors, spreadsheets applications, and presentations applications.

ii. Billing
   - Applications designed to monitor and manage customer billing. This is determined by users' system usage and subscriptions/licensing to products and services.

iii. Customer Relationship Management (CRM)
   - Call-center applications.

iv. Financials
   - An application used for data analytics, tracking and reporting financial activities, including the processing of expenditure, generating invoices, payroll, and managing taxes.

Platform-as-a-Service (PaaS)

For this service model, the cloud provider is responsible for consumer access to the development tools and services used to build and deliver their applications. (Cisco NetAcad, 2019)

It offers development services and a platform (e.g., comprising of a database, middleware, and development tools) in which custom applications are built and developed without requiring additional software installation and hardware requirements which saves cost. PaaS has built-in tools that cover security and web services interfaces for the applications that are being built. Applications developed under PaaS can be integrated with applications internally and with other applications outside of its local network. (Odun-Ayo, Ananya, Agono, & Goddy-Worlu, 2018)

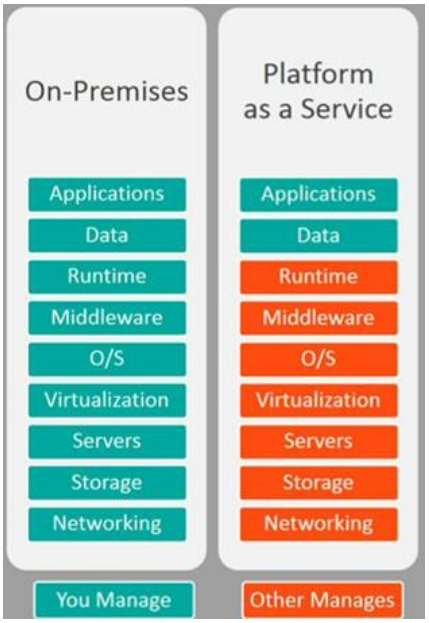

Figure 15 - Platform-as-a-Service (PaaS)
(Watts & Raza, 2019)

Examples of PaaS:

i. Business Intelligence
   - Optimize business processes by creating a platform to develop systems to resolve business issues

ii. Database
   - Provide access to data/information needed to deliver business operations

iii. Application Development and Testing
   - Development of application(s) required and needed by organizations

iv. Integration
   - Integrated solutions and applications between different platforms and networks

Infrastructure-as-a-Service

For this service model, the cloud provider is responsible for access to the network resources, virtualized/non-virtualized network services, and supporting/maintaining the network infrastructure. (Cisco NetAcad, 2019)

The main components of this services model are the delivery of servers, storage, compute resources and network interconnectivity. With IaaS, it allows providers to control and maintain activities in the cloud/data centers while allowing users the flexibility to deploy and manage virtual instances of services themselves based on specific needs. The provider only manages the compute, storage, network, and other related virtualization resources needed for users to have access to a virtual environment in which they can have access and deploy their customized applications. (Odun-Ayo, Ananya, Agono, & Goddy-Worlu, 2018)

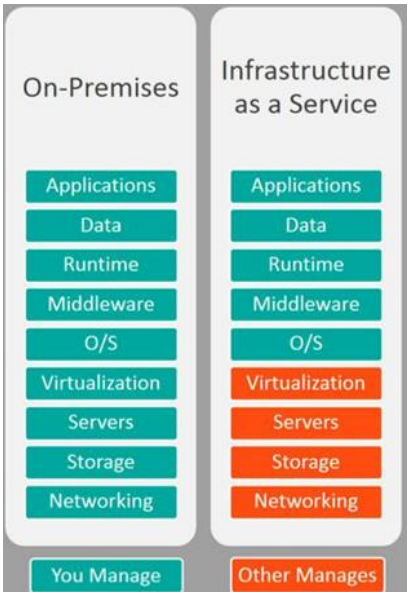

Figure 16 - Infrastructure-as-a-Service (IaaS) (Watts & Raza, 2019)

Examples of IaaS:

i. Content Delivery Networks (CDNs):
   - Caches user content and files to improve the system performance such as speed and the cost associated with the delivery of web contents on other systems (e.g., websites and mobile applications)

ii. Backup and Recovery:
   - The ability for continuous backup and seamless recovery of files.

iii. Compute:
   - Involves server requirements for maintaining cloud systems and performing the actual processing of applications

iv. Storage:
   - Involves storage ability useful for recording activities of applications and files to be used during application processing, backup, and recovery purposes

The figure below describes and summarizes these Cloud Service types. It should be noted that each type of service will have different scopes of responsibilities relative to the customers and service providers. Stack components in which vendors have the responsibility will have more content as customers utilized services from IaaS, PaaS, and SaaS, respectively.

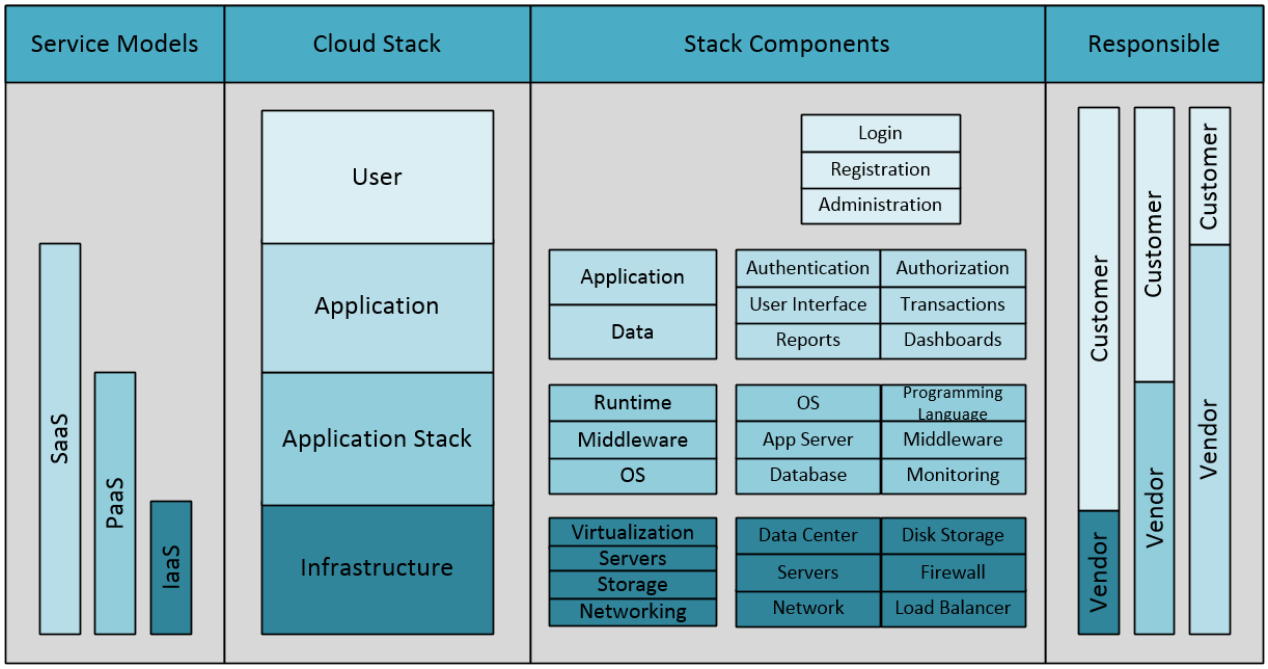

Figure 17 - Summary of Service Models and its Cloud Stack Components (Kavis, 2018)

Aside from these core service models, there are other types of models that are available to customers as a service in the context of cloud computing. Newer services are being offered to consumers as cloud technologies are continuously evolving. The following are some of these services that are focused on a specific service requirement: (Wikipedia, 2019)

Service	**Acronym**
Analytics as a service	AnaaS
Artificial intelligence as a service	AIaaS
Business process as a service	BPaaS
Content as a service	CaaS
Database as a service	DBaaS
Disaster Recovery as a service	DRaaS
Distribution as a service	DaaS
Energy storage as a service	ESaaS
Games as a service	GaaS
IT as a service	ITaaS
Logging as a service	LaaS
Management as a service	MaaS
Mobility as a service	
Monitoring as a service	
Machine Learning as a service	MLaaS
Network as a service	NaaS
Recovery as a service	RaaS
Search as a service	SaaS
Security as a service	
Storage as a service	
Transportation as a service	TaaS
Testing as a service	TaaS
Unified Communications as a Service	UCaaS

Table 1 - Other flavors of features offered to customers as a service

This paper will only be discussing and referring to the core service models highlighted in the previous sections as these other services are derived from these core models.

Cloud Infrastructure Deployment Models

There are four primary cloud infrastructure models, as shown in the figure below.

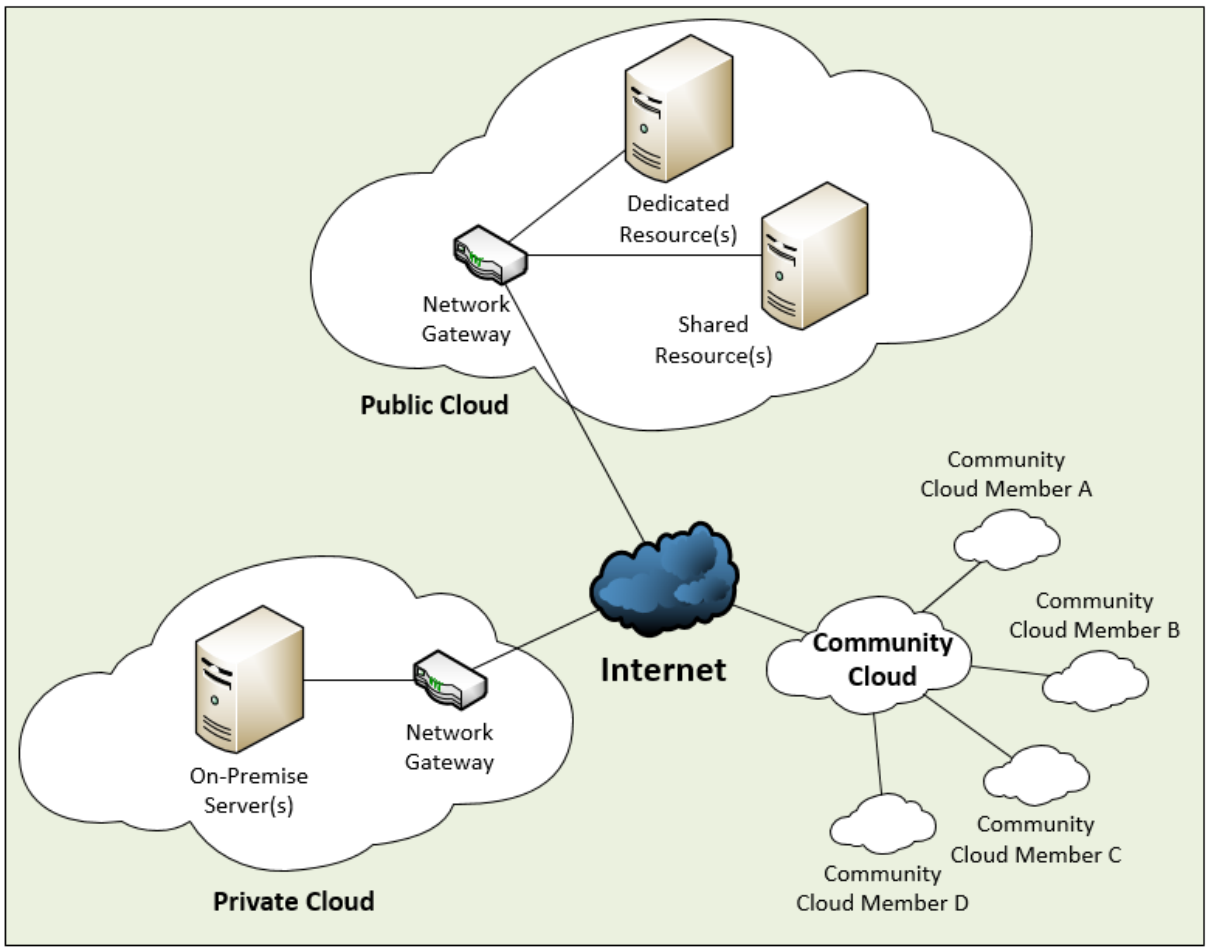

Figure 18 - A typical Hybrid Cloud Topology

Public clouds

A cloud infrastructure that offers applications and services to the public consumers through the Internet, which could be either be free or are offered on a pay-as-you-go model. (Odun-Ayo, Ananya, Agono, & Goddy-Worlu, 2018)

Private clouds

This cloud infrastructure is setup using an organization's private network which is intended for private use. Capital and high on-going costs are required in order to build and maintain this type of infrastructure. External organizations can also manage it through strict security access. (Odun-Ayo, Ananya, Agono, & Goddy-Worlu, 2018)

Community clouds

This is an exclusive cloud infrastructure used by a specific community. A community in this context refers to multiple organizations that have functional needs that have been customized to serve these various networks and their requirements. For example, healthcare organizations must remain compliant with policies/laws and must secure the transfer of information between multiple private networks and the community network. (Odun-Ayo, Ananya, Agono, & Goddy-Worlu, 2018)

Hybrid clouds

Hybrid Cloud is a cloud infrastructure that consists of two or more clouds (e.g., a combination of either Public, Private, and Community Clouds). Each part remains a distinct abstraction to resolve an organization's requirements but are connected within this single hybrid framework. Based on user privileges, users would have multiple degrees of access to multiple services found within a specific hybrid cloud infrastructure. (Odun-Ayo, Ananya, Agono, & Goddy-Worlu, 2018)

Federated Clouds

Another type of cloud infrastructure is called Federated Cloud. It is a hybrid cloud setup where different cloud providers agreed to combine their cloud infrastructures enabling easy sharing to resources among consumers. This, however, is not included in the NIST classification of cloud deployment and infrastructure types. (Odun-Ayo, Ananya, Agono, & Goddy-Worlu, 2018)

Comparison: Private vs. Public Cloud

Relative to a user, a Cloud is an interconnection of several devices that offers business solutions within an organization (HCL, 2019). Special considerations are made in order to design an effective model that will provide optimized, secure, and high availability of processes and other services that comply with several legal guidelines and with the organization's business requirements. Based on the advantages and disadvantages of these Cloud Architectures, organizations tend to leverage these factors to their advantages while considering value propositions and trade-offs.

Private Cloud

Private Cloud is a cloud environment wherein major cloud architecture components are purchased, set-up, and managed on-premise or is hosted by a third-party service provider which is typically servicing a single dedicated client or organization. The term "Private" refers to the fact that this architecture is not being shared with others. Private Cloud is typically used by mid- to large-size organizations seeking more control over their environment. With greater control and visibility, organizations can operate with compliance-sensitive business processes, ensuring security and performance. It is, however, the responsibility of the organization to perform all management, maintenance, and updates of all resources used within this type of architecture. (Akamai, 2019; Microsoft Azure, 2019; Owen, 2019; Tsang, 2019; Raza, 2018; White, 2014)

Advantage	Description
Improved Security	Higher control to management and security is possible as resources are not shared with others.
Compliance	Compliance with stringent regulations as organizations can run protocols, configurations, and measures to customize security based on unique workload requirements.
SLA	High SLA performance and efficiency.

Table 2 - Advantages of Private Cloud
(Akamai, 2019; Microsoft Azure, 2019;
Owen, 2019; Tsang, 2019; Raza, 2018; White, 2014)

Disadvantage	Description
Cost	Higher starting capital and sustainability costs compared with other cloud services for short-term applications. Scaling will also be costly.
Access	Due to high-security measures, access mediums (i.e., mobile phones) may have limited capabilities within a private network.
Technology	The on-premise data center may not offer high scalability to meet with the ever-changing and unpredictable demands for such computing resources.
Inelastic	An organization cannot readily customize and scale its system environment once all resources have been installed to meet unpredictable demands.

Table 3 - Disadvantages of Private Cloud
(Akamai, 2019; Microsoft Azure, 2019;
Owen, 2019; Tsang, 2019; Raza, 2018; White, 2014)

Suitable for:
Highly regulated agencies (e.g., industries and government).
Any organization that needs high-security management and control over its business processes and underlying computing infrastructure
Any organization that has the capital to invest in high-performance technologies and has the human resources to perform its setup and maintenance

Table 4 - Use case for Private Cloud
(Microsoft Azure, 2019;
Owen, 2019; Tsang, 2019; Raza, 2018)

Public Cloud

Public Cloud is a cloud environment consists of services that are availed off by the organizations and are delivered via the Internet from these third-party providers. These services do use Cloud Infrastructure resources that are external to the organization. All services and resources are managed, developed and maintained by the third-party services providers (i.e., depending upon which service model is being utilized) and are expected to provide these services under the SLAs (Service Level Agreements). As the provider delivers most services, all management tasks and costs for these resources are minimized. Essentially, it is an extension of an organization's network and service environment. (Akamai, 2019; Microsoft Azure, 2019; Owen, 2019; Tsang, 2019; Raza, 2018; White, 2014)

In a public cloud, organizations share the same cloud infrastructure resources with other organizations or cloud "tenants." However, some services offer dedicated solutions if stricter security requirements are required. Unlike that of Private Cloud, in which capital cost is a primary factor in establishing an organization's cloud infrastructure, Public Cloud offers a pay-as-you-go model such that the only cost is the usage that has been incurred during a specific billing period, virtually eliminating the upfront high capital expense. (Microsoft Azure, 2019; Raza, 2018)

Advantage	Description
Lower costs	There is no initial investment needed to deploy and setup the computing infrastructure. Since a consumer only pays for what they used for, there is no need to purchase any hardware or software. Cloud services offer different and flexible pricing models that have different SLA offerings. This provides the ability to focus on delivering initiatives aiming to develop and optimize internal processes.
No maintenance	There is a reduced requirement for technical experts for computing resources as the cloud service vendors are responsible for the maintenance and management of this infrastructure.
Near-unlimited scalability	On-demand resources are available to meet business requirements.
High reliability	A vast number of servers are run and managed by the cloud service mitigates risk from device failures.
Utility Model	Cloud providers provide a pay-as-you-go payment model, which is an economical way to go if the organizations are spinning up and tearing down development servers regularly.
No Contracts	Along with the utility model, organizations are only paying by the hour – if they want to shut down the server after only 2 hours of use, there is no contract requiring the ongoing use of the server.

Self Managed	As the cloud service providers service these resources, and once the consumer avail of these cloud services, this pay-as-you-go payment model provides a platform to self-manage these systems based on its organizational requirements but can be a disadvantage if consumers do want a fully-managed solution which could be limited for some cloud services.

Table 5 - Advantages of Public Cloud
(Akamai, 2019; Microsoft Azure, 2019;
Owen, 2019; Tsang, 2019; Raza, 2018; White, 2014)

Disadvantage	Description
Cost Increase	For medium- to large-sized enterprises, the total cost of ownership (TCO) can rise exponentially.
Not as secure as private	Since it is a Public Cloud, this would not be the most viable solution for real-time and mission-critical business workloads.
Less Control	It may not suffice with some regulatory compliance (i.e., dependent on regulatory body and industry) as it has low infrastructure visibility and control.
Shared Hardware	Since multiple tenants are using the public cloud environment, computing resources (i.e., hardware and software applications) are shared across the infrastructure.

Table 6 - Disadvantages of Public Cloud
(Akamai, 2019; Microsoft Azure, 2019;
Owen, 2019; Tsang, 2019; Raza, 2018; White, 2014)

Suitable for:
Unpredictable computing needs, such as communication services for a sudden spike in network traffic
Applications and services critical to perform business and computing workloads
Variable demands in computing resources due to its on-demand setup and availability
Development and UAT (User Acceptance Test) environments

Table 7 - Use case for Public Cloud
(Microsoft Azure, 2019; Owen, 2019; Tsang, 2019; Raza, 2018)

Various Public Cloud platforms are available in the market today. This includes some of the most prominent cloud players in the market, namely Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. Section 3 will provide a high-level overview and discussion of these major Public Cloud Service Providers.

The Need for a Hybrid Setup

While projecting the optimal environment for an organization based on requirements remains "cloudy," current trends show the growth of cloud computing and its adoption within organizations. In general, organizations seek solutions that enable efficient and effective process execution on locations that make the most sense for specific resources relative to an organization's needs, a trend that is increasingly involving public cloud services for its delivery. Most organizations consider several issues from these requirements when deciding which deployment model to use including the following: (Kulikova & Sturrus, 2014)

i. Cost benefits provided by different providers;
ii. Reliability and performance benefits;
iii. Deployment speed;
iv. Storage location (for example, the data protection laws governing the local jurisdiction);
v. Security, risk, and control concerns; and,
vi. Availability of off-the-shelf, ready-to-use cloud solutions.

As more organizations recognize the potential of implementing a hybrid cloud environment in their system, the need for a Hybrid Cloud design best approach is needed. Strategic questions such as to what extent should an organization incorporate hybrid systems, how to maximize the benefits of multiple cloud environments, and most importantly, how these services would support their business requirements must be considered all together with Hybrid Cloud Architecture design and deployment.

In order to approach and maximize the features of a hybrid setup, organizations should also align themselves with some of the traditional cloud design and deployment frameworks that can be utilized, such as the Amazon Well-Architected Framework, Microsoft Solutions, and Operations Framework, and the Zachman Framework. These frameworks are used to evaluate the hybrid design and optimize it to deliver business needs appropriately.

This paper is about Hybrid Cloud Architecture Design, Deployment Models, and Analysis. It aims to provide an overview of what networking and what a computing system is, and who are the cloud "actors" involved in these processes and explain their roles, specifically with Cloud Service Providers.

By developing this Hybrid Cloud Architecture Design, Deployment, and Analysis documentation, it is intended to be used as a basic template in designing an actual hybrid cloud environment for an organization. In this paper, it includes three (3) detailed example of pseudo-organizations having different sizes, business requirements, and computing systems. Computing system design and analysis will be performed using select services from three (3) of the most popular Cloud Service Providers in today's market, namely Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP). The end of this documentation will also give a conclusion and other recommendations

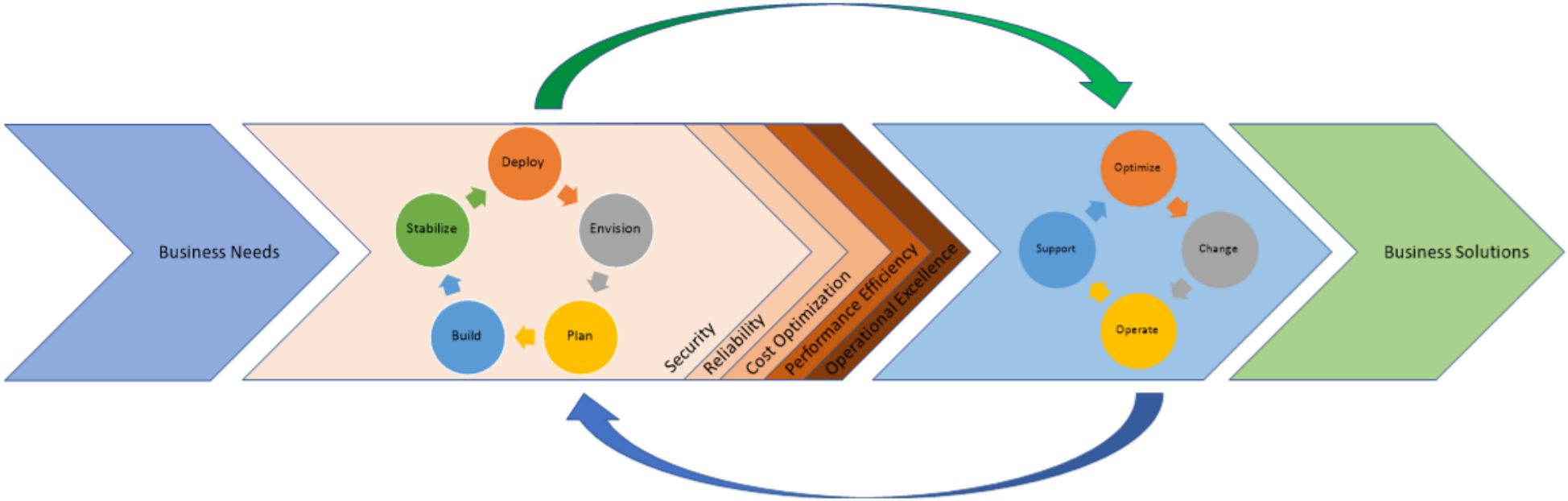

Figure 19 – Hybrid Cloud Design and Deployment Adoption from Amazon and Microsoft

Amazon`s Well-Architected Framework is based on five pillars, namely operational excellence, performance efficiency, cost optimization, reliability, and security, and provides a platform to evaluate architecture design and implement services that are scalable and robust. The framework has been developed to help designers build and create a secure and efficient infrastructure to support an organization`s needs (AWS - Architecture, 2019). Microsoft Solutions Framework delivers a proven practice for planning, building, and deploying technology solutions and provides a standard based on proven best-practices and approaches (Microsoft - MSF, 2004). On the other hand, Microsoft Operations Framework delivers practical guidelines for everyday IT practices that integrate management, governance, and compliance activities that help organizations establish a reliable and cost-effective computing system (Microsoft - MOF, 2008). By combining these frameworks and implementing it in this study, all resources related to these frameworks can be utilized and apply them to the design and deployment of a Hybrid Cloud Architecture.

A more sophisticated framework for Enterprise Architecture, such as the Zachman Framework, considers all factors from the Executive, Business, Technical and Operations level, its process flow and could provide answers regarding questions about the interrogatives “Who”, “What”, “Where”, “When”, “Why” and “How” which enables a comprehensive and composite description of ideas through reification via Identification, Definition, Representation, Specification, Configuration, and Instantiation. (Zachman, 2008)

Section 3: The Hybrid Cloud

Hybrid Cloud Architecture

Hybrid Cloud is a cloud environment that offers "the best of both worlds" of features from Private Clouds and Public Clouds. In a Hybrid Cloud, data and application can move between these two (2) different cloud architectures for greater flexibility and deployment options. An example of this integrated infrastructure would be to deploy a high-volume, low-security compliant service in a Public Cloud while core-sensitive, business-critical processes are performed in the Private Cloud. Another instance in which a Hybrid architecture will be useful is when an organization's core business processes are performed in the Private Cloud, but an aperiodic increase in cloud infrastructure resource demand due to an increase in user traffic in which a Public Cloud is needed to support these processes. (Akamai, 2019; Microsoft Azure, 2019; Owen, 2019; Tsang, 2019 Raza, 2018; White, 2014)

Advantage	Description
Control	It provides an environment to host a private infrastructure for critical and sensitive information.
Flexibility and Scalability	Organizations can take advantage of additional resources in the public cloud on-demand. Scalability is delivered without compromising data security and availability.
Cost-effectiveness	With the ability to scale to the public cloud, organizations pay for extra computing power only when needed.
Ease	Cloud migration can be done gradually by phasing in workloads overtime on the cloud.
Policy Compliance	Policy-based workload distribution across public and private infrastructure environments based on security, performance, and cost requirements.
Reliability	High reliability as the services is distributed across multiple data centers across public and private data centers.
Security	Improved security on computing environments such that sensitive workloads can be performed on-premise while regular processes can be performed in the cloud
Hybrid Deployment	High-speed applications (e.g., database services) can be integrated (i.e., in terms of hardware) with the private cloud, which combines the performance of both the on-premise and cloud computing resources. This can be done on-demand based on business needs and other related requirements.

Table 8 - Advantages of Hybrid Cloud
(Akamai, 2019; Microsoft Azure, 2019;
Owen, 2019; Tsang, 2019; Raza, 2018; White, 2014)

Disadvantage	Description
Cost-effectiveness	It can get expensive.
Resource Compatibility required	Services and resources utilized between the hybrid environments must have strong compatibility and integration.
Complexity	Complexity is introduced as an organization has to manage and orchestrate an evolving and hybrid combination of public and private cloud infrastructure.

Table 9 - Disadvantages of Hybrid Cloud
(Akamai, 2019; Microsoft Azure, 2019;
Owen, 2019; Tsang, 2019; Raza, 2018; White, 2014)

Suitable For:
Organizations that need compliance with various security, regulatory and performance requirements, and parameters
Fully utilizing hybrid cloud environments without compromising its value proposition
Improving security on existing cloud solutions such as SaaS offerings that must be delivered via secure private networks.
Strategically reaping the benefits and trade-offs between the best cloud service available and selecting them based on business requirements (e.g., cost, functionality, and agility)

Table 10 - Use case for Hybrid Cloud
(Microsoft Azure, 2019;
Owen, 2019; Tsang, 2019; Raza, 2018)

Proper consideration must be addressed to optimally acquire and balance the advantages and disadvantages of this type of architecture. A correct understanding and evaluation of any business requirements can help with the selection of needed computing requirements, improve computing system design, and allow insights on how to adjust the deployment models based on the computing requirements. These steps deliver a great platform in which analysis can be readily performed to improve further and optimize the services provided by this hybrid computing environment.

For Hybrid Cloud Architecture, proper consideration of where data must be stored and where the applications must be hosted should be established between the Private and Public Cloud Architecture concerning business and computing requirements. Aside from fundamental design principles, several factors should be considered before implementing a Hybrid Architecture which could include: (Tsang, 2019)

1. Business Requirements
   This is an organization's specific computing and other technological needs.
2. Capital and Costs
   This is how organizations are willing to spend upfront and periodically.
3. Legal Compliance
   This is what rules or standardization an organization needs to comply with based on which industry and federal body it is engaged in.
4. Setup and Management
   This refers to the complexity, setup requirements, and the type of management procedures the organization is willing to perform.
5. Engineering Time
   This refers to the time the company is willing to spend on the overall setup and management.
6. Licensing
   This refers to how external vendor companies charge for the services performed by their devices utilized by end-users/organizations either with on-premise or cloud solutions.
7. Data Availability (HA)
   This refers to maintaining the high availability of services and information by providing backup and recovery sites in case of computing failures.
8. Disaster Recovery (DR)
   This refers to the ability of an organization to seamlessly react against a disaster without profoundly affecting services provided by their organization.
9. Security
   This refers to the capability of an organization to provide security capabilities encompassing all variables within the organization, such as data, applications, device, access, user controls, physical security, and others.

Once a correct understanding of all the business and computing parameters have been addressed and evaluated, the proper design shall be delivered. Designing a hybrid system will involve several essential designs and implementation principles. This typically involves trade-offs between several factors to optimize the cost, device complexity, service performance, maintenance, and others. These factors are as follows: (Giraldeau, 2019)

Key Design Principles

1. Reliability
   Ability of the system to deliver highly available services to the intended consumers.
2. Scalability
   Ability of the system to adapt to the demand for change within the computing requirements of the intended consumers.
3. Flexibility
   Ability of the system to adjust based on the consumer's needs, change in business models, technology trends, and competition among other organizations.
4. Efficiency
   Ability of the system to utilize all resources (i.e., For On-Premise: Electrical (Power) and Mechanical (Cooling); For Cloud: Compute Management (Instance execution as it is normally charged as a pay-as-you-go model) to provide a cost-effective setup.
5. Modularity
   Ability of the organization to organize resources and categorized them into different "silos" in order to create a holistic view of the computing resources needed to provide services to the consumers.
6. Standardization
   Policies must be established to enable organizations to optimize processes and align them with any procedures related to these computing resources all based from organizational policies in compliant with industry standards of management and standardization (e.g., NIST, ITIL, COBIT, and ISO)

Cloud Systems

Private Cloud Technology

In a Data Center design, the most critical components are Physical Infrastructure, Compute, Storage, Networking, and Management. The physical infrastructure consists of all resources that support all other computing elements in the data center, namely mechanical (i.e., Cooling Systems) and electrical (i.e., Power Distribution Systems). Compute are the resources performing the actual application and data computation, which are typical running through virtualization. Storage will provide the data storage for all systems in the data center network, which typically works with controllers and cache locations to optimize and secure its data availability. This also includes Database services that allow a more efficient application execution. Network, including Security, is the component that securely connects all resources to efficiently deliver network and data traffic inbound and outbound of that specific data center. Lastly, Management and Governance initiatives, which are mostly based on frameworks such as NIST, ITIL, COBIT, and ISO, are critical to manage and standardize the day-to-day process within the data center. (Giraldeau, 2019)

In order to manage an on-premise private cloud environment, computing resources must be purchased and set up to meet its business requirements. The core elements, as discussed, are the Compute, Network, Security, Storage, and Database which are offered by numerous organizations providing solutions to these components. This paper will be limited to only using hardware and software features offered by the following companies to provide an On-premise / Private Cloud environment.

1. Dell
   Dell is a multinational computing technology company that leads business innovation through developing technologies to support the evolving IT landscape. (Dell, 2020). For this paper, we will be utilizing its Dell PowerEdge suite of servers to provide computing resources for hosted applications delivered through Hypervisors.
2. VMware
   WMware is a global leader in cloud infrastructure & digital workspace technology which accelerates digital transformation for evolving IT environments (VMware, 2020). For this paper, we will be utilizing its VMWare ESXi, which is a Type 1 Hypervisor capable of running VMs which are running different sets of operating systems (e.g., Windows and Linux)
3. NetApp
   NetApp is a computing technologies organization that specializes in data storage hardware and associated management software. (Techopedia, 2020). For this paper, we will be utilizing its NetApp FAS storage systems which offer the best performance for its cost and flexibility as well as a power range of other features to help reduce complexity and increase efficiency. (NetApp, 2020)

4. Cisco
   Cisco is the worldwide leader in networking for the Internet. They offer several solutions such as routers, switches, and other networking and security appliances which will be utilized in this paper.
5. Oracle
   Oracle is one of the largest vendors in the enterprise IT market, with databases and database management systems as their flagship products. For this paper, we will be using Oracle Database as the database component for a private cloud system. (Rouse, Stedman, Lavery, Sirkin, & Kruggel, 2017)

Licensing

For consumers to realize the full features of their purchased products, a license must also be purchased for these products. Licensing could include added device features, full use of hardware and software, client support, and others. As there are several licensing schemes that technology companies offer to their clients, the following are the most common types of these licensing systems:

Processor-Based Licensing

Processor or Core-based is a licensing wherein an unlimited number of users are permitted to access the product, provided that the number of cores running the product (i.e., a software product) will not exceed the cores permitted and identified at the time of purchase. (Maloy, 2012)

Client Access Licensing

Client Access or User-based licensing is a licensing wherein the named Authorized Users enable to use of the product must not exceed the number of licensed acquired at the time of purchase. (Maloy, 2012)

Licensing for Support

Licensing for support is an additional service purchased for a product that enables organizations with external support regarding that specific product from when the license has been activated until its expiration period. This is especially helpful when on-premise personnel are not experts for that specific product line, and external support is needed.

APIs

API (Application Programming Interface) is an interface between applications. An example of this would be a website application that pulls information from a map service hosted through another application. APIs simplifies processes for developers since it reduces time to create an interface between different applications, it adheres to most web standards (i.e., HTTP and REST), and they are more standardized in terms of security, monitoring, management, and governance. (MuleSoft, 2020)

This is especially important with networking and connecting applications within a Hybrid Cloud Infrastructure. However, these features will not be discussed in full detail for this study.

Public Cloud Technology

In order to create a computing system from external resources, the utilization of public cloud services must be considered. This removes the load from managing, developing, and maintaining the computing infrastructure in compliance with Service Level Agreements (SLAs) and focuses only on the setup, utilization, and execution of service-oriented activities.

For this study, the paper utilizes cloud services and features from three (3) of the most popular cloud service providers in today's market, namely Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

Public Cloud Service Providers

Most Cloud Service Providers has several deployment schemes for their services, which include IaaS (Infrastructure as a Service), SaaS (Software as a Service), and PaaS (Platform as a Service). Several public cloud service providers offer dedicated hosting, co-located, and public hosted environments such as Oracle Cloud Infrastructure (OCI), Telus IT & Cloud Services (Telus CIDC), and others. However, for this documentation, this paper will be focusing only on the three (3) most prominent players in today's public cloud market.

Amazon Web Services (AWS)

Amazon Web Services is a subsidiary of Amazon providing on-demand and pay-as-you-go cloud computing services to individuals and organizations. AWS offers cloud computing web services that provide a set of abstract infrastructure and distributed computing building blocks and resources. This is currently the most popular and mature cloud service provider in the market today. (Wikipedia, 2019)

The following factors must be first considered before going into the technical details of what services does it provide to its consumers.

AWS Location

AWS spans 22 Regions having multiple Availability Zones (AZs) (69 in total). They also have 210 Point of Presence (PoP) or Edge Locations for Content Delivery to its End-users. This global infrastructure serves 245 countries and territories in total and is planning to expand more by adding more Regions and AZs in the future. (AWS - Global Infrastructure, 2019)

Figure 20 - AWS Geographical Locations
(AWS - Global Infrastructure, 2019)

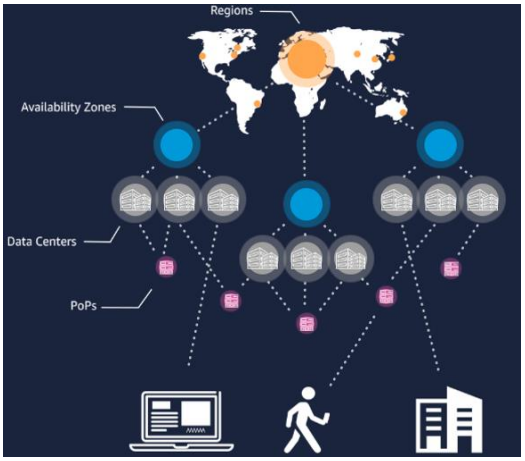

Figure 21 - Regions, Availability Zones and Point of Presence
(AWS - Global Infrastructure, 2019)

For more details regarding the AWS location, please refer to the AWS Global Cloud Infrastructure Documentation.

AWS Security Model

AWS Security Model is a shared responsibility between its consumers. AWS assumes the responsibility of the operation, management, and control of the components down to its physical security. On the other hand, the consumers assume the responsibility of all service resources that it will utilize, including but not limited to updating security patches, configuration, and access controls to these resources. (AWS - Shared Responsibility Model, 2019)

For more information regarding AWS Security Model, please refer to AWS Shared Responsibility Model Documentation.

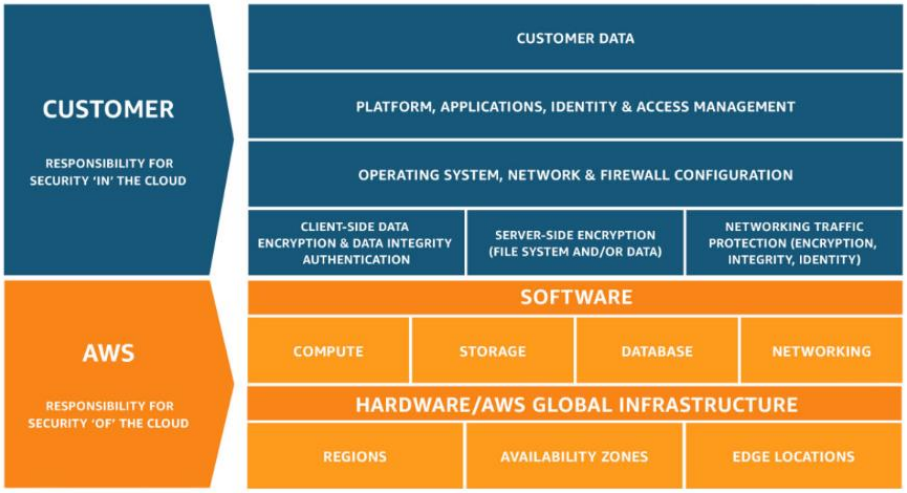

Figure 22 – AWS Shared Responsibility Security Model
(AWS - Shared Responsibility Model, 2019)

AWS Compliance Offerings

AWS has several compliance standards certified Globally and in the United States, Canada, Asia Pacific, and Europe. It is also aligned with laws, regulations, and compliant with several standardizations and compliance frameworks in the industry.

For more information regarding AWS Compliance Offerings, please refer to the AWS Compliance Programs Documentation.

AWS Cost

AWS has a tool to calculate the Total Cost of Ownership (TCO) of running applications with AWS and compare it with On-Premise or Collocation Services.

For more information regarding the Pricing Calculator, please refer to the AWS Estimate Tool.

For more information regarding the Comparison Calculator, please refer to the AWS TCO Tool.

AWS SLAs

Service Level Agreements (SLAs) are the representation of the service providers' commitment to its consumers, particularly on all the services it provides. For AWS, most of the services follow the same service commitment and service credit schemes.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.9% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

Figure 23 - Most common AWS SLAs
(AWS - Service Level Agreements, 2019)

However, for compute services, its SLA service credit percentage is at 30% instead of 25%.

For more information regarding the Compute SLAs, please refer to the AWS Compute SLA Documentation.

For more information regarding all other SLAs, please refer to the AWS SLA Documentation.

AWS Services

For more information regarding all the services offered by AWS, please refer to the following documentations:

- AWS Documentation
- AWS Cloud Products

Microsoft Azure (Azure)

Microsoft Azure is a subsidiary of Microsoft providing cloud-computing services for building, testing, deploying, and managing applications/services through its infrastructure. Microsoft Azure offers reliable integration with its Microsoft set of utilities for further improve services to individuals and organizations. (Wikipedia, 2019)

The following factors must be first considered before going into the technical details of what services does it provide to its consumers.

Azure Location

Azure spans 55 Regions having multiple Availability Zones (AZs). This global infrastructure serves 140 countries in total and is planning to expand more by adding more Regions and AZs in the future. (Azure - Global Infrastructure, 2020)

Figure 24 - Azure Geographical Locations
(Azure - Global Infrastructure, 2020)

For more information regarding Azure locations, please refer to the Azure Global Infrastructure Documentation.

Azure Security Model

Azure Security Model is a shared responsibility between its consumers. Azure assumes the responsibility of the physical host, data center management, and networking. On the other hand, the consumers assume the responsibility of its data, endpoint resources, accounts, and access management. Some other responsibilities vary based on the service type. (Azure - Security, 2019)

For more information regarding Azure Security Model, please refer to Azure Shared Responsibility in the Cloud Documentation.

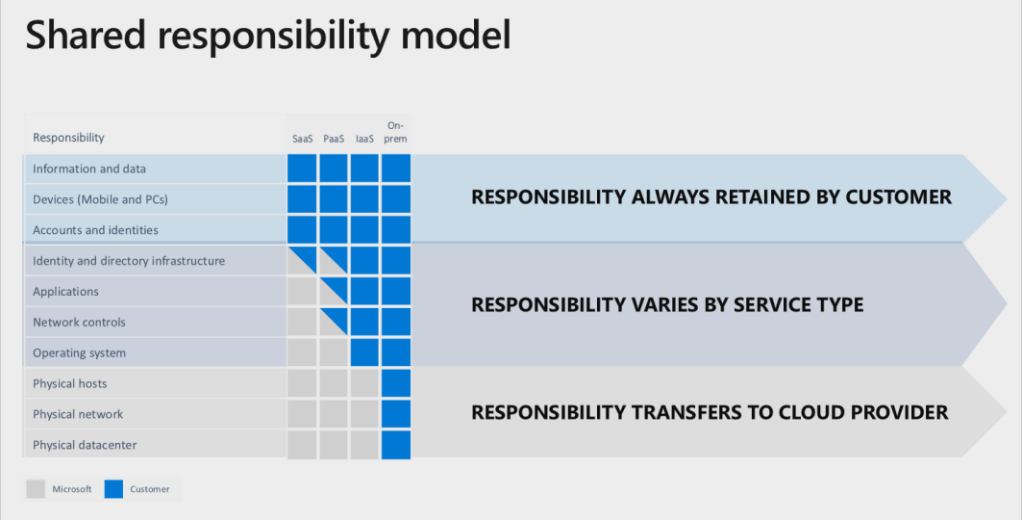

Figure 25 – Azure Shared Responsibility Security Model (Azure - Security, 2019)

Azure Compliance Offerings

Azure has several compliance standards certified Globally, Regionally (e.g., US Government), and other Industry-based compliance offerings.

For more information regarding Azure Compliance Offerings, please refer to the Microsoft Compliance Offerings Documentation.

Azure Cost

Azure has a tool to calculate the Total Cost of Ownership (TCO) of running applications with Azure and compare it with On-Premise Workloads.

For more information regarding the Pricing Calculator, please refer to the Azure Pricing Calculator.

For more information regarding the Comparison Calculator, please refer to the Azure TCO Calculator.

Azure SLAs

Service Level Agreements (SLAs) are the representation of the service providers' commitment to its consumers, particularly on all the services it provides. For Azure, most of the services follow a distinctive service commitment and service credit schemes.

For more information regarding the Azure SLAs, please refer to the SLA Summary for Azure Services Documentation.

Azure Services

For more information regarding all the services offered by Azure, please refer to the Azure Products documentation

Google Cloud Platform (GCP)

Google Cloud is a platform offered by Google, providing a suite of cloud computing services such as management tools. Compared with the first two (2) service providers, this is the newest addition to the market of cloud service providers. (Wikipedia, 2019)

The following factors must be first considered before going into the technical details of what services does it provide to its consumers.

GCP Location

GCP spans 20 Regions having multiple Availability Zones (AZs) (61 in total). They also have 134 Point of Presence (PoP) or Edge Locations for Content Delivery to its End-users. This global infrastructure serves 200+ countries in total and is planning to expand more by adding more Regions and AZs in the future. (GCP - Cloud Locations, 2020)

Figure 26 - GCP Geographical Locations
(GCP - Cloud Locations, 2020)

For more information regarding GCP locations, please refer to the GCP Cloud Locations Documentation.

GCP Security Model

GCP Security Model is an end-to-end process. GCP assumes the responsibility for securing the infrastructure, information, application network and implementing and reviewing Google's security policies. Some other responsibilities vary based on the service type. (GCP - Google Security Overview, 2020)

For more information regarding GCP Security Model, please refer to Google Security Overview Documentation.

GCP Compliance Offerings

GCP has several compliance standards certified Globally and in the United States, Canada, Latin America, Asia Pacific, and Europe. It is also aligned with laws, regulations, and compliant with several standardizations and compliance frameworks in the industry.

For more information regarding GCP Compliance Offerings, please refer to the GCP Compliance Resource Center Documentation.

GCP Cost

GCP has a tool to calculate the cost of running applications and services with GCP.

For more information regarding the Pricing Calculator, please refer to the GCP Pricing Calculator.

GCP SLAs

Service Level Agreements (SLAs) are the representation of the service providers' commitment to its consumers, particularly on all the services it provides. For GCP, most of the services follow the same service commitment and service credit schemes.

Monthly Uptime Percentage	Percentage of the monthly bill for the Covered Service that will be credited to future monthly Customer bills
99% to < 99.9%	10%
95% to < 99%	25%
< 95%	50%

Figure 27 - Most common GCP SLAs
(GCP - Service Level Agreements, 2020)

However, for some services, its SLA service credit will provide additional days of operation or free of charge usage, which is dependent on the monthly uptime percentage.

For more information regarding the GCP SLAs, please refer to the GCP SLAs Documentation.

GCP Services

For more information regarding all the services offered by GCP, please refer to the Google Cloud Platform Services Summary documentation

On-Premise and Cloud Services

In summary, the following are the resources and cloud services that will be utilized in this paper:

On-Premise Computing Resources

- VMWare ESXi
- NetApp FAS
- Oracle Database
- Cisco Appliances

Cloud Services

The following items were primarily considered for this study. Please do note that only a select number of cloud services have been ultimately selected. Only the most generic services (i.e., highlighted from the list) were selected to generalize and narrow down this study. For more information regarding these selected services, please refer to the Appendix – Public Cloud Services Section of this documentation.

Cloud Service Provider	Basic Compute	Containers	Serverless	Batch Processing	App Hosting
Amazon Web Services	**EC2**; Lightsail; VMware Cloud on AWS	ECS; EKS; ECR; Fargate	Lambda; Serverless Application Repository	Batch	Elastic Beanstalk
Microsoft Azure	**Virtual Machines**; Virtual Scale Sets	AKS; Container Instances	Functions	Batch	App Service; Service Fabric; Cloud Services
Google Cloud Platform	**Compute Engine**	Kubernetes Engine; Knative	Cloud Functions	N/A	App Engine

Table 11 - Compute Services

Cloud Service Provider	Block Storage	File Storage	Object Storage	Hybrid Storage	Archival Services	Disaster Recovery
Amazon Web Services	**EBS**	**EFS**	**S3**	Storage Gateway	**Glacier**	**CloudEndure**
Microsoft Azure	**Block Blob Storage**	**File Storage**	**Blob Storage**; Queue Storage; Data Lake Store	StorSimple	**Backup**	**Site Recovery**
Google Cloud Platform	**Persistent Disk**	**Cloud Filestore**	**Cloud Storage**	N/A	**Cloud Storage**	N/A

Table 12 - Storage Services

Cloud Service Provider	Virtual Private Cloud	Lease Line Services	Content Delivery	DNS
Amazon Web Services	**VPC**	**Direct Connect**	**CloudFront**	**Router 53**
Microsoft Azure	**Virtual Network; VPN Gateway**	**ExpressRoute**	**CDN**	**Azure DNS**
Google Cloud Platform	**Virtual Private Cloud; Cloud NAT**	**Cloud Interconnect**; Network Service Tiers	**Cloud CDN**	**Cloud DNS**

Table 13 - Networking Services

Cloud Service Provider	Relational/SQL Database	NoSQL Database	In-Memory Database
Amazon Web Services	**RDS;** Aurora; Neptune	**DynamoDB**	Elasticache
Microsoft Azure	**SQL Database**; Database for MySQL; Database for PostgreSQL; Server Stretch Database; Data Factory	**Cosmos DB**; Table Storage	Redis Cache
Google Cloud Platform	**Cloud SQL**; Cloud Spanner	**Cloud Bigtable; Cloud Datastore**	N/A

Table 14 - Database Services

Cloud Service Provider	Application Lifecycle Management	Cloud Monitoring	Cloud Management
Amazon Web Services	CodeStar; CodePipeline	**CloudWatch; CloudTrail**	**Systems Manager;** Management Console; Auto Scaling; Elastic Load Balancing
Microsoft Azure	Visual Studio Team Services; Visual Studio App Center	**Monitor; Log Analytics**	Portal; **Policy; Cost Management**
Google Cloud Platform	N/A	**Stackdriver**	**Stackdriver**

Table 15 - Monitoring and Management Services

Cloud Service Provider	Security	Authentication and Access Management
Amazon Web Services	**GuardDuty; Macie; Shield; WAF**	**IAM; Directory Service; Organizations; Single Sign-On**
Microsoft Azure	**Security Center**	**Active Directory**; Multi-Factor Authentication
Google Cloud Platform	**Cloud DLP; Cloud Security Scanner**	**Cloud IAM; Cloud IAP**

Table 16 - Security and Access Management Services

Cloud Service Provider	Migration
Amazon Web Services	**AWS Database Migration; AWS Migration Hub; AWS Server Migration Service; AWS Snowball; AWS Snowball Edge; AWS Snowmobile**
Microsoft Azure	**Azure Migrate; Azure Site Recovery; Azure Database Migration Services; Data Box**
Google Cloud Platform	**Transfer Appliance; Transfer Service**

Table 17 – Migration Services

Cloud Service Provider	Big Data Analytics
Amazon Web Services	Athena; EMR; Kinesis; Redshift
Microsoft Azure	HDInsight; Stream Analytics; Data Lake Analytics; Analysis Services
Google Cloud Platform	Cloud Dataflow; Cloud Dataproc

Table 18 - Data Analytics Services

Cloud Service Provider	Machine Learning	Cognitive Services	IoT	AR & VR	3rd Party Software and Services	Training	Support
Amazon Web Services	SageMaker; AML; Apache MXNet on AWS; TensorFlow on AWS	Comprehend; Lex; Polly; Rekognition; Translate; Transcribe	IoT Core	Sumerian	Marketplace	Training and Certification	Support
Microsoft Azure	Machine Learning	Cognitive Services	IoT Hub; IoT Edge	N/A	Marketplace	Training	Support
Google Cloud Platform	Cloud Machine Learning Engine	Cloud Natural Language; Cloud Speech API; Cloud Translation API; Cloud Video Intelligence	Cloud IoT Core	N/A	Cloud Launcher; Partner Directory	Training Programs	Support

Table 19 - Other Services

Assumptions and Limitations

As the documentation is limited in nature, there are some constraints and assumptions made to deliver the discussion points for scenarios produced in this paper.

The following are the assumptions and limitations of this study:

- All business requirements utilized for these scenarios are only high-level ones. Please do note that some services needed to deliver business requirements that are mentioned in this document would not be covered in full detail. Additional details for these services will be added through hyperlinks.
- The documentation will only consider the high-level design and deployment models that can be used as a basic template for designing a Hybrid Cloud Environment. Specific configuration, setup, and maintenance of these services will not be explicitly covered in this documentation.
    - This documentation aims to provide the answers to the “Why”s of Hybrid Cloud Design and Deployment and not with the “How”s.
- Management and governance policies such as NIST, ITIL, COBIT, and ISO will not be fully discussed in these scenarios.
- APIs and improved storage and database types will not be discussed in this study.
- Not all on-premises and cloud services would be discussed in full detail for this documentation. The focus will be given on IaaS, PaaS, and SaaS service offerings.
- Only specific on-premise vendor products specified on this documentation will be used as part of business requirement delivery for these scenarios.
- The location of data centers within each region would contain multiple redundant zones.
- It should be assumed that the availability of the CSPs utilized for this study is at 99.9%.
- General and select cloud services (i.e., from a variety of more specialized services) will be utilized for each CSPs to deliver business requirements on these scenarios.
- The construction of the Indonesia Regional Database for AWS and GCP has been completed.
- Legal compliance and guidelines used to align with business requirements that are used in this documentation will be highlighted but will not be explained in full detail.
- All costs utilized within this documentation is taken from the time of writing, February 9, 2020, and could have been changed going forward.
    - For more updated pricing information, please refer to Section 3: Public Cloud Service Provider under Services. From there, refer to the pricing documentation of the selected service.
- Cloud services used for this study’s cost analysis have standard, balanced, and premium features with additional sub-features that can be leveraged off. In this study, Standard and Balanced services have been selected for each scenario.
    - It should be noted that there are special cost policies per each service sets depending on the location, operation, data size, data rate, and the type of resources that will execute or host a cloud service to be utilized.
- To simplify cost analysis performed on these scenarios, some pricing details for cloud services with no per-month obligations will be set to a per-month setup.

Section 4: Business Modeling and Scenarios

This section will provide comprehensive scenarios on how a Hybrid Cloud Architecture could be implemented, and what general factors should be considered to design, deploy, and deliver their business and computing needs.

As highlighted in the previous section, the system's design should reflect all information regarding the organization in order to support all its required business data usage and application processes. Several aspects should be considered in designing a Hybrid Cloud Architecture. This could include the following[1]:

1. Understand and capture all relevant information regarding the organization, such as:
    a. Scope of Work/Industry;
    b. History; and,
    c. Size and Demographics.
2. Define its business requirements;
3. Consider data and application location;
4. Establish the total capital and costs;
5. Identify legal compliance guidelines based on industry relevance;
6. Finalize the computing systems security to:
    a. Provide data and application availability;
    b. Establish disaster recovery strategies;
    c. Implement an identity and access management policies;
    d. Deliver penetration security;
7. Finalize any licensing that needs to be done regarding applications and services used on-premise or through the cloud;
8. Know how to proceed with the setup and management of the system; and,
9. Estimate the time it would take to complete the project.

The following examples will utilize this high-level approach[2] together with all the best approaches presented in this documentation on how to design and efficiently deploy services within a Hybrid Cloud Environment. This paper describes three different pseudo-organizations with varying business requirements that require a Hybrid Cloud Environment implementation to, ultimately, provide and deliver its business services to its clients.

[1] For Items For items 6 and 7, proper key design principles must be considered which have been highlighted in the previous section.

i. Service Reliability
ii. System Scalability and Flexibility
iii. Overall Efficiency
iv. Process Modularity
v. Standardization

Items 5, 6d, 7, 8, and 9 will be covered but will not be discussed in full detail as this is out of scope for this paper.

[2] Please do note that this won't cover the detailed steps on how to perform specific configurations with the on-premise and cloud services that will be used for this documentation. This documentation is meant to answer the "why" and not the "how".

Small Business Model

This section provides a high-level discussion regarding all business and computing requirements for a Small Business Organization. The paper aims to show an all-purpose template to capture all factors relevant within the organization and to ultimately utilize this information to design and deploy its Hybrid Cloud Architecture.

Overview

Organization Name: Pearson and Harvey Barrister
Industry: Law
Location: Toronto, Ontario
End Users: 10 – No IT Personnel

The organization, Pearson and Harvey Barrister, is a Law Office that just transferred to a new office location and will be requiring assistance to migrate their small network infrastructure to this new location. The migration will involve the transfer of end-devices, installation of an entirely new data cable infrastructure, and to optimize their network environment relative with their previous old office setup. Since they are in the Law industry, data redundancy regulations require that all their data must only be stored within Canada.

It also requires a website solution to host their web application environment to cater to their clients online by introducing their services and publishing a calendar for each lawyer for appointment requests.

Topology

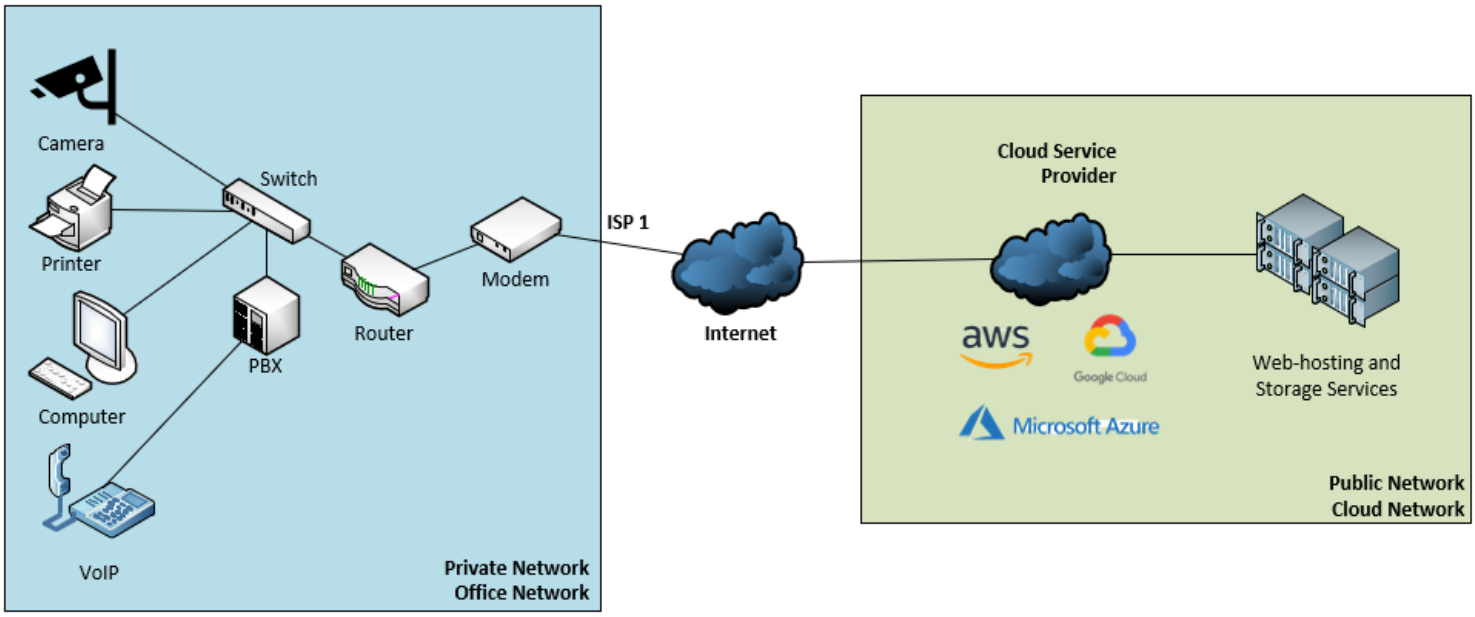

Figure 28 – Small Business Network Topology

Requirements

Summary Requirements:

The summarized requirements for the organization are as follows:

a. Data residency guidelines for the organization requires that all data should only be located in Canada
b. Provide the organization with a secure and reliable Internet connectivity
c. Equip the organization with high data availability and simple disaster recovery features
d. Consideration is made by the organization to utilize centralized cloud services from a CSP to deliver its web-hosting and storage services
e. LAN and WAN Networking
    - LAN
        i. VoIP Systems
        ii. Centralized Printer Systems
        iii. Security Cameras
        iv. End-Point Security
        v. Centralized Storage System
        vi. Intermediary Device and Device Management
        vii. DHCP Server
        viii. Identity and Access Management
    - WAN
        i. Internet Connectivity
        ii. SaaS
            - Email Services
            - Document Processing Tool(s)
        iii. VPN Server
        iv. Web Hosting
        v. Remote Cloud Storage

Requirement Details[3]:

LAN:

- VoIP Systems
  - This service will include an Intercom/Automatic Attendant and Call Queueing
  - It is preferred to have a PSTN/Analog line device rather than a PoE VoIP device
- Centralized Printer Systems
  - Network Printer(s) to be mapped to all end-user devices within the network
- Security Cameras
  - These are preferred to be delivered through PoE
  - All footage will be stored on a local hard-drive device and the cloud as a backup
  - The security feeds of the camera should be accessible through:
    - Mobile App
    - Website
- End-Point Security
  - Anti-malware programs will be installed in all end-user devices within the organization
- Centralized Local Storage (i.e., NAS)
  - Network folders are to be made available and mapped for other end-users within the network
- Intermediary Device and Device Management
  - On-premise devices should able to deliver the LAN infrastructure and be able to easily managed for maintenance and monitoring activities
  - This could include the following resources:
    - Switches
    - Routers
    - Security Appliances
    - Other critical Data Center components
- DHCP Server
  - This service will provide automatic IPv4 Address, default gateway, and DNS settings for the local network
- VPN Server
  - Hosted locally and is used by VPN Clients to connect to the local network through the Internet
- Identity and Access Management System
  - This service will authenticate security requests within the organization.

[3] Due to the limited scope of this study, it should be noted that these requirements will not be covered in full detail. Moreover, additional external resources will be provided for these undiscussed topics.

WAN:

- Internet Connectivity
  - Only one (1) connection to an Internet Service Provider (ISP) is required
- SaaS
  - Managed externally by a SaaS provider
  - The required applications include the following:
    - E-mail
    - Document Processing Tool
- Web Hosting
  - The organization is planning to refresh its branding by creating a new website that will cater to its client's needs
- Remote Cloud Storage
  - As part of the organization's efforts to implement data redundancy, the remote cloud storage contains all backup of all files used by the users
  - Syncing of backup files is done continuously and is hosted within the same province in compliance with data residency requirements

Cloud Solutions

The following services taken from AWS, Azure, and GCP will be used for this section of the study. These services have been taken from the services highlighted in Section 3 and were selected to satisfy the requirements for this Small Business Model. Please note that these selected services could be further filtered based on the business requirements. For more information regarding these selected services, please refer to the Appendix section of this documentation.

Cloud Service Provider	Authentication and Access Management
Amazon Web Services	**IAM; Directory Service; Organizations; Single Sign-On**
Microsoft Azure	**Active Directory**; Multi-Factor Authentication
Google Cloud Platform	**Cloud IAM; Cloud IAP**

Table 20 – Small Business – Summary: Security and Access Management Services
This will be used to provide security and access management to the organization

Cloud Service Provider	Basic Compute
Amazon Web Services	**EC2**; Lightsail; VMware Cloud on AWS
Microsoft Azure	**Virtual Machines**; Virtual Scale Sets
Google Cloud Platform	**Compute Engine**

Table 21 – Small Business – Summary: Compute Services
This will be used to satisfy the web hosting for the organization

Cloud Service Provider	File Storage	Object Storage	Archival Services	Disaster Recovery
Amazon Web Services	**EFS**	**S3**	**Glacier**	**CloudEndure**
Microsoft Azure	**File Storage**	**Blob Storage**; Queue Storage; Data Lake Store	**Backup**	**Site Recovery**
Google Cloud Platform	**Cloud Filestore**	**Cloud Storage**	**Cloud Storage**	N/A

Table 22 – Small Business – Summary: Storage Services
This will be used to satisfy the storage requirement of the organization

Cloud Service Provider	Cloud Monitoring	Cloud Management
Amazon Web Services	**CloudWatch; CloudTrail**	**Systems Manager;** Management Console; Auto Scaling; Elastic Load Balancing
Microsoft Azure	**Monitor; Log Analytics**	Portal; **Policy; Cost Management**
Google Cloud Platform	**Stackdriver**	**Stackdriver**

Table 23 – Small Business – Summary: Monitoring and Management Services
This will be used to monitor and manage the cloud service utilized by the organization

CSP Services

As the general requirement, the organization needs to provide a secure and reliable network that would provide high data availability and satisfy the required data residency guidelines posted by their industry bodies. The organization will also require Business Continuity (BC) and Disaster Recovery (DR) Strategies to continue with business processes in case of a natural, technological, or man-made disaster(s).

Basic Requirements

Several computing and other technological requirements have been highlighted. These include VoIP, Printer, and Camera Systems. For these requirements, the organization could require an on-premise solution and would typically involve buying VoIP devices and a VoIP communications server, which can be run as a VM instance or run as a standalone server. An example would be the Cisco Unified Communications Manager, Elastix, Avaya, and other on-premise solutions. However, there are also cloud solution implementations that would be able to provide these features such as the Amazon Connect, Microsoft Business Voice, and Google Voice.

For small businesses, Printer and Camera systems would be installed on-premise. Printers will be connected via TCP/IP, and appropriate drivers will be installed to user workstations dependent on the type of printer is being installed. Camera systems will be connected to a video recording device on-premise, with an option to transfer the files through file transfer protocols and storage solutions available within the cloud.

Another requirement highlighted was End-Point Security. For small businesses, this will involve purchasing licenses to stand-alone anti-malware software, which will be installed directly to each user-workstations.

Intermediary devices must be set up to establish the LAN network. Devices required include Cisco routers, switches, access points, and relevant security appliances. The routers will provide appropriate DHCP services for the LAN, and the security appliances will provide on-premise security against malware and would provide VPN access for remote users outside the organization. A local centralized storage system would also be installed using NAS solutions such as the NetApp FAS Storage Systems.

Finally, a secure and reliable Internet connection must be obtained from an Internet Service Provider (ISP) for the organization to connect to the WAN network, and ultimately, access cloud services to set up the organization's Hybrid Cloud Architecture. DNS server access should also be requested from the ISP if available. However, there are also cloud solution implementations that would provide DNS features such as Amazon Route 53, Azure DNS, and Cloud DNS or from third-party DNS service providers such as Cloudflare.

Cloud Requirements

After capturing the overall information regarding the organization, consideration must be made for the most critical requirements that will require Cloud Services namely the E-mail Services, Document Processing Tools, Identity and Access Management, Web Hosting and Remote Storage Systems which will support the business processes, operation continuity and disaster recovery procedures.

E-mail service (SaaS) is a critical tool within organizations to send-out and receive messages to and from external organizations. This tool is often integrated with Calendaring and Collaboration services within an application running these services. AWS, Azure, and GCP have created solutions for these services, namely the AWS WorkMail, Microsoft Exchange, and Google Mail[4].

Document Processing Tools (SaaS) are applications that allow users to create human-readable files. The most popular tools in today's market are Microsoft Office and Google Drive Services[5].

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Productivity Service	Amazon WorkMail	Microsoft Exchange and Office	G Suite
Plan	-	Office 365 Business Premium	Business
Cost	$4 per user	$16 per user	$15.6 per user
Data Residency	US	Most Critical Applications located in Canada, with some minor services stored in the US	US
Features	Provides Email services and some Microsoft Service Integration	Includes most critical Productivity applications and some Management Features	Includes most critical Productivity applications, Security and Management Features
Dedicated Mobile Applications	None. Uses Web applications.	Yes	None. Uses Web Applications.

Table 24 – Small Business: Productivity Services

[4] It should be noted that Microsoft Exchange and Google Mail is the most mature E-mail Services available in the today's market. Organizations will be able to leverage all the integrations available for this service to other compatible services.

[5] Together with all other productivity tools such as E-mails, Calendars and Document Processing makes up Office 365 or Microsoft Suite (i.e., Microsoft) and G Suite (i.e., Google).

Identity and Access Management (I&AM) (SaaS) is the ability of the system to provide access classification to users within the organization. There are several services offered in the cloud by various CSPs. The following CSP and I&AM services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Small Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Authentication and Access Management Service	I&AM	Active Directory	Cloud IAM
Cost	Free	Free	Free
Data Residency	US	US/CA	US/CA
Availability	99.90%	99.90%	99.95%

Table 25 – Small Business: Authentication and Access Management Services

Web Hosting (IaaS/PaaS) will require a VM instance to host and run the website and its web embedded application. Website hosting will require an appropriate address and name translations via DNS services. These DNS Services could include Amazon Route 53, Azure DNS, and Cloud DNS. Aside from DNS services from CSPs, there also various DNS services offered by third-party organizations such as Cloudflare. There are other Webhosting solutions dedicated to providing this service, which is offered by CSPs. Such services include Amazon Lightsail, Azure Web Apps, and GCP App Engine. The following Compute and DNS services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Small Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Compute Service	EC2	Virtual Machines	Compute Engine
Cost	Customizable depending on the design	Customizable depending on the design	Customizable depending on the design
Data Residency	US/CA	US/CA	US/CA
Availability	99.99%	99.95%	99.99%

Table 26 – Small Business: Compute Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
DNS Services	Route 53	Azure DNS	Cloud DNS
Cost	**DNS Server**: $0.5 per hosted zone/month **Queries**: $0.4 per million req/month for the first billion req	**DNS Server**: $0.64 per zone/month for first 25 **Queries**: $0.512 per 1st million req/month	**DNS Server**: $0.2 per zone/month for first 25 **Queries**: $0.4 per million req/month for the first billion req
Data Residency	US/CA	US/CA	US/CA
Availability	100.00%	100.00%	100.00%

Table 27 – Small Business: DNS Services

Storage systems (IaaS) are critical for the organization's business continuity and disaster recovery strategies. It enables the organization to continue business operations in case of natural or man-made disasters affecting the corporate environment. For Small Businesses, File and Object storage solutions are applicable. File Storage presents information as multiple levels of files organized in folders. On the other hand, Object Storage stores data and associates it with its corresponding metadata. (Red Hat, 2020). As discussed in the previous sections, File Storage is best used for regular local enterprise file and storage services, while Object Storage is best used for cloud integrations since it primarily uses APIs and metadata to handle data queries. For this organization, it will be utilizing the File Storage solution to satisfy its requirements since there are no significant and fast data access requirements for the organization that can be provided by Block Storage and that no other critical applications will utilize cloud storage and API storage integrations through the Object Storage.

Archival systems (IaaS) are also part of the organization's storage systems. This solution enables organizations to store files that will be left unaccessed for long periods due to the organization's data archival guidelines in compliance with industry standards. As the organization will only require access to this remote storage location in case of a disaster, this remote storage is sufficient enough as its DR strategy. The following Storage services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Small Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
File Storage Service	EFS	File Storage	File Store
Cost	$0.3 per GB/month	$0.27 per GB/month	$0.2 per GB/month
Data Residency	US/CA	US/CA	US/CA
Availability	99.90%	99.99%	99.90%

Table 28 – Small Business: File Storage Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Archival Services	Glacier	Backup (Blob)	Cloud Storage
Cost	**Storage**: $0.004 GB/month **Upload**: $0.05 per 1000 request **Upload Requests** **Retrieval**: $0.01 per GB Data **Transfer**: $0.02 per GB	**Storage**: $6.4 (base payment up to 50 GB) + $0.0287 per GB + Blob Storage Operational Costs **Operations**: $0.09 per 10,000 Requests	**Storage**: $0.026 GB/month **Operation**: $0.05 per 10,000 Operations **Retrieval**: $0.01 per GB **Transfer**: $0.12 per GB
Data Residency	US/CA	US/CA	US/CA
Availability	99.99%	99.90%	99.95%

Table 29 – Small Business: Archival Services

In order to have real-time information regarding all the cloud resources utilized by the organization, Cloud Monitoring, and Management services (SaaS) should also be considered. This is useful for monitoring the cloud computing systems' health, determining diagnostic information, and troubleshooting should there be any issues within these resources. The following Cloud Monitoring and Management services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Small Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Cloud Monitoring Services	CloudWatch; CloudTrail	Monitor; Log Analytics	Stackdriver
Cost	**CloudWatch**: $0.3 per metrics/month **CloudTrail**: $2.1 per 100,000 events	$2.76 per GB after 5GB	**Logging**: $0.5/GiB **Monitoring**: $0.151/MiB **API Monitoring**: $0.01/1,000 requests
Data Residency	US/CA	US/CA	US/CA
Availability	99.9%, 99.9%	99.90%	99.95%

Table 30 – Small Business: Cloud Monitoring Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Cloud Management Services	Systems Manager;	Policy; Cost Management	Stackdriver
Cost	**OpsItems**: $2.97 per 1000 issues **Requests**: $0.039 per 1,000 requests	Free	**Logging**: $0.5/GiB Data **Monitoring**: $0.151/MiB **API Monitoring**: $0.01/1,000 requests
Data Residency	US/CA	US/CA	US/CA
Availability	99.90%	No SLA	99.95%

Table 31 – Small Business: Cloud Management Services

Analysis

Based on this small business model, the on-premise requirement for the organization are all about end-user devices in which they will have direct interaction with throughout their day-to-day business operation. This is true for any organization as these are the interface that provides access to more complex services available locally or remotely.

For this model, a LAN, Wireless LAN, and Cloud Services comprise this Hybrid Cloud Architecture. It is more efficient and secure to implement separate network access for the corporate LAN and the public LAN such that a separate network domain can be established, which minimizes any risks within the small organization. There are, however, more advanced devices and services that the organization can utilize. Nevertheless, it will be excessive as the organization would not be able to utilize its full capabilities, and it would be costly. Cloud services such as AWS Cloud Backup and Sync, Azure OneDrive, and GCP Backup and Sync will enable devices within smaller organizations to backup data from their local machines into the cloud at limited to no cost. However, more robust storage solutions will be utilized for this organization.

Wireless LAN is utilized within the organization to access any content within the Internet. As this is a discrete network domain, there is some separation between devices within the organization's LANs, so any issues from one LAN will not affect the other.

Aside from the cloud storage requirements of the organization, it will also utilize web-hosting services, I&AM, storage, DNS pointers, and cloud service monitoring and management. These private and public solutions would be sufficient and will enable the organization to perform its daily business processes.

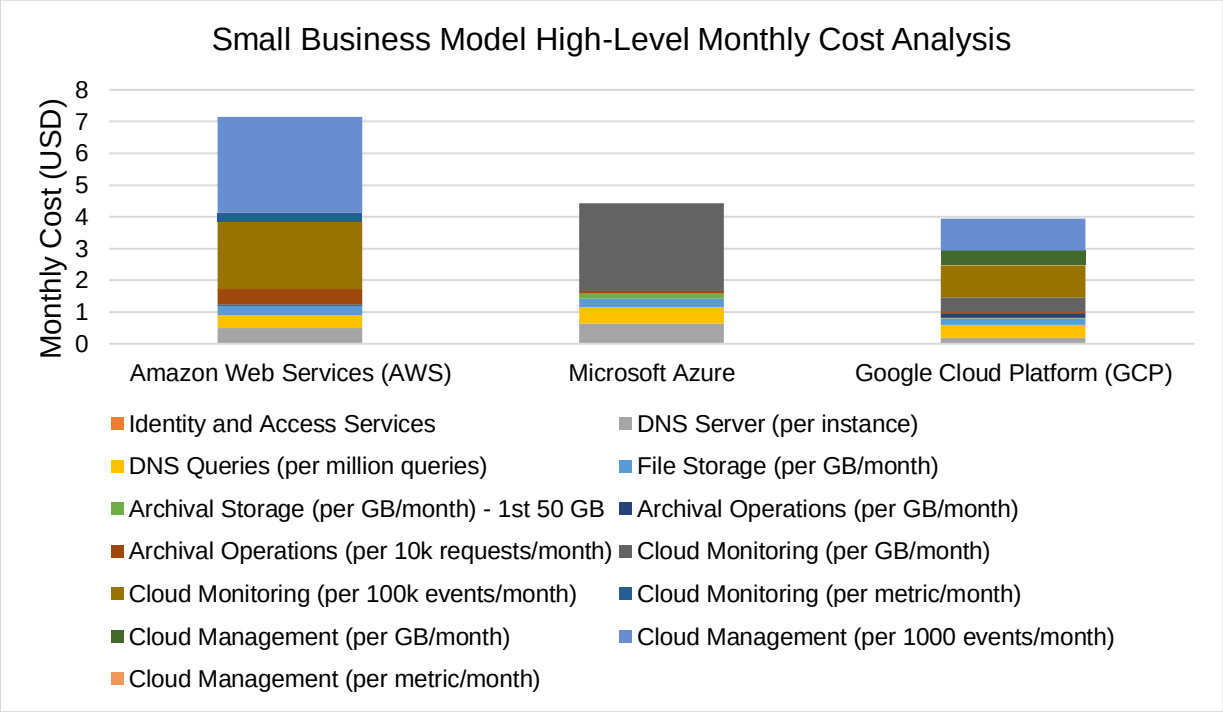

Figure 29 - Small Business Cost Analysis

For this analysis, cost information regarding Productivity Tools has been removed to primarily focus on other critical services to be utilized from these CSPs. Security services have also been removed since basic security services considered for AWS in this documentation offer more features compared with Azure and GCP, which will effectively reflect higher costs for AWS relative to both Azure and GCP[6].

Based on the graph relating to the organization's monthly cost, it could be seen from this high-level cost analysis that if these cloud services are compared, AWS has the highest cost for the organization's requirement implementation. This is primarily brought by the following factors:

- The services selected for this study to deliver the requirements[7];
- The pricing of the services at the time of writing the documentation; and,
- The cost of utilizing Cloud Management and Monitoring Services (i.e., highest cost contributor for all CSPs).

To even more save costs, the organization could consider removing monitoring tools since resources that will be utilized under their cloud environment are only the web hosting instance and the storage service. For this high-level cost analysis, preference could be given for both Microsoft Azure and GCP to implement their web hosting requirement (excluding productivity tools). Location, for which the service stores its information to deliver its actual services, should also be considered for these services. Based on the provided information above, all services considered from these CSPs are hosted in Canada, satisfying the data residency requirements of the organization.

Furthermore, it should be noted that the organization is looking for centralized management and utilization of cloud services from a CSP (through the local CSP region in only one availability zone). As the organization's primary business workflow will involve document and productivity tools, a centralized solution through one (1) CSP will be selected such that it will provide powerful services to deliver this primary productivity tool(s) requirement, without compromising the other requirements highlighted in this documentation. With this analysis, the organization will select a Microsoft Suite environment since it offers multiple tools to allow productivity within the organization. Applications can be installed and run natively into any user workstation, compared with G Suite, which is limited only with browser-based applications. Since the most services that will be offered and used by the organization is using a pay-as-you-go model, no complex licensing processes must be made, which aids with managing all the services and related subscriptions to such services. Furthermore, the deployment of services relating to workstations (i.e., Storage and I&AM Services) will be easier since workstations within the organization will be mostly running the Windows OS, which all belong in the Microsoft suite of products and services.

[6] For the pricing information of these services, please see the CSP Services section of this Small Business Modeling and Scenario.
[7] It should be noted that services selected are ranging from Standard and Premium services. Most services also have added capabilities which will incur additional costs. For this study, most services selected utilized Standard Features. All prices denoted are in USD.

It should be noted that not the best services must be used in a hybrid cloud architecture implementation as there are also several factors outside of the scope of this study that affects the selection of cloud services in any organization. Appropriate frameworks, such as the combined AWS and Microsoft architecture framework can be used to streamline further and enhance the efficiency of the operations going forward.

Medium Business Model

This section provides a high-level discussion regarding all business and computing requirements for a Medium Business Organization. The paper aims to show an all-purpose template to capture all factors relevant within the organization and to ultimately utilize this information to design and deploy its Hybrid Cloud Architecture.

Overview

Name: The Tech Guys
Industry: Software/Health Care
Location: Edmonton, Alberta
End Users: 50
Departments: 7

The organization has only implemented an on-premise solution to support their day-to-day business processes. However, initiatives to improve business operations were established, and by this, a total overhaul of its IT department was made. With this new leadership in the IT department, the CIO aimed to optimize the business operations, reduce costs, and minimize risks regarding on-premise resource failure(s) by implementing cloud solutions.

The current setup was made such that applications and storage, both for development and production, are only hosted on-premise, and data are automatically backed up through external hard drives and manually through tape drives daily.

1. For its previous Disaster Recovery strategies, these drives are removed from the on-premise site by the end of the day and are stored in an external bank locker and kept by the Senior IT staff for safekeeping.

The future state of the setup is to create a Hybrid Cloud Environment such that:

1. The production network will be hosted in the selected CSP while the local network of the organization will serve as its redundant site;
2. Application, Storage, and Database environments used on-prem for its web-based application will be replicated and hosted through an IaaS provider as an alternate site;
    i. In order to optimize its storage and database environments, proper consideration of which storage and database solution and deduplication strategies shall be selected
    ii. The application (i.e., Front-facing web portals and mobile applications for clients) will have a transactional and reporting functionality and will be implemented a separate function to improve business process performance
3. Application, Storage, and Database environments are to be built on a development platform delivered through a PaaS provider;
4. The cloud network environment will be optimized by availing other SaaS solutions to streamline business processes;
5. The Storage Environment will also be improved by provisioning an on-premise device that is compatible with the CSP devices to perform file mirroring/backup and recovery relevant for DR initiatives.

Third-party systems solution providers previously installed the organization's data center environment. As the IT staff of the organization is limited, they will be utilizing support from third-party organizations such as these system solution providers and technical solution experts from purchased on-premise devices.

Part of the organization's business department works with the Provincial Government of Alberta. Thus, as an organizational standard, all information must be residing within only in Alberta, Canada. All services should also follow any guidelines related to the Provincial Government's Information and Technology standards so that policy alignment must be established.[8]

Topology

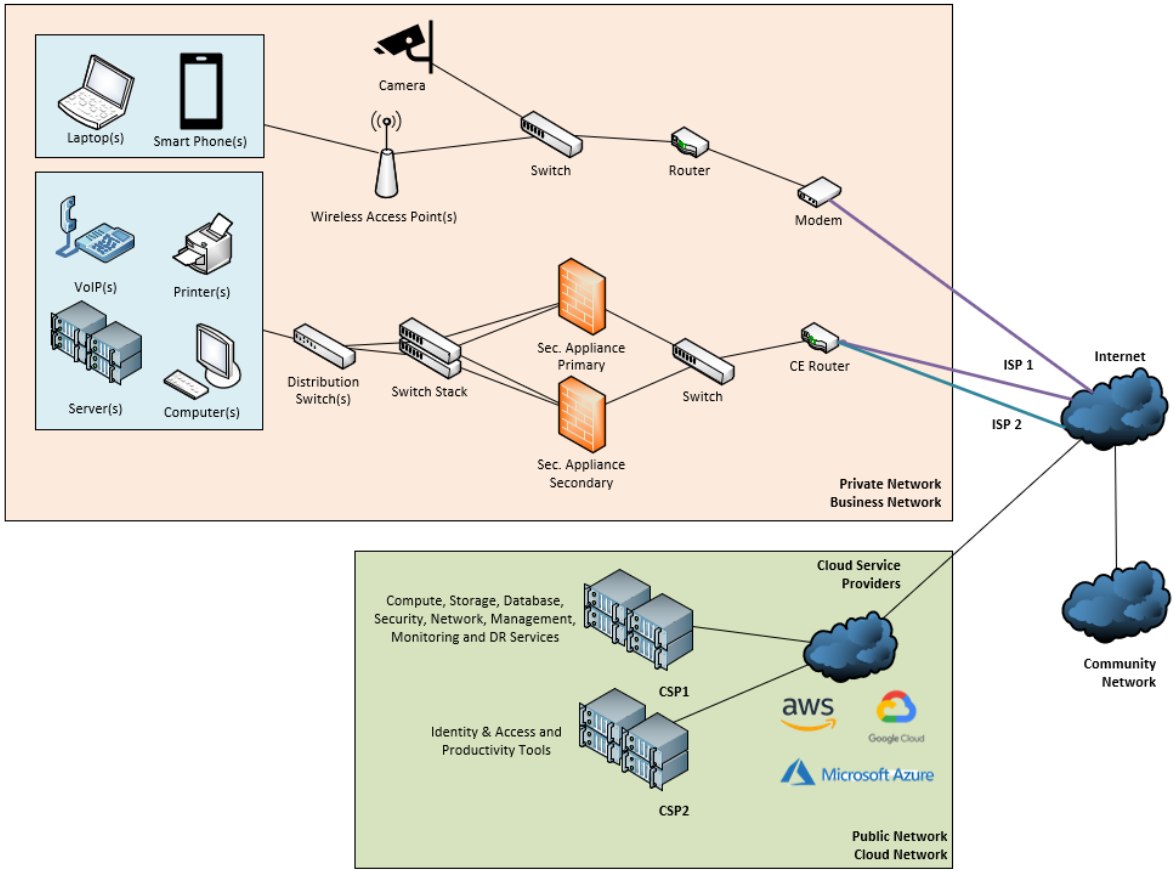

Figure 30 - Medium Business Network Topology

[8] Please do note that this guideline alignment will not be discussed in full detail for this documentation.

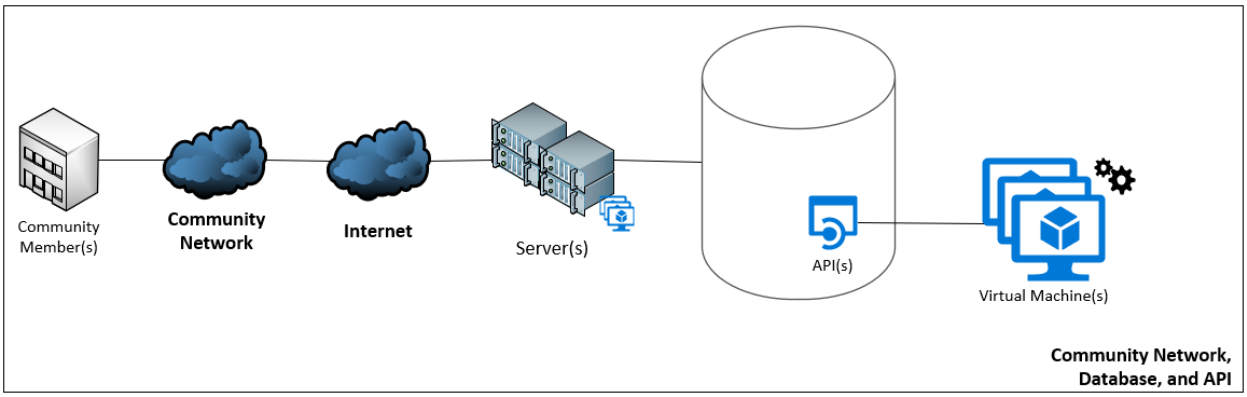

Figure 31 - Community Network Topology and Setup

Connection to Community networks are necessary to align with some legal regulations within a specific industry (i.e., Health Care, Government, Etc.)

- The on-premise server hosted with VMs will “register” and connect to the community network
- Server “buckets” queue requests and appends to the database instances with API “collaborating” with other “Process VM instances”
- “Process VM instances” executes, coordinates with API and submits the result to a server connected to the community network

Requirements

Summary Requirements:

The summarized requirements for the organization are as follows:

a. Data residency guidelines for the organization requires that all data should only be located in Canada
b. Provide the organization with a secure and reliable Internet connectivity
c. Equip the organization with high data availability, device and link redundancy, and disaster recovery features
d. Create separate modules for application transactional and reporting processes
e. Establish a connection to Community networks
f. Setup data synchronization between the on-premise cloud and the public cloud
g. LAN and WAN Networking
    - LAN
        i. VoIP Systems
        ii. Printer Systems
        iii. Security Cameras
        iv. End-Point Security/Anti-Malware Server
        v. Intermediary Devices Management
        vi. VPN Server
        vii. LAN Optimization
            - Network Subnetting and VLANs
            - Private and Public LANs
            - Separate Network Environments
                - Production
                - UAT
                - Development
            - Network Security
        viii. Server Setup and Data Synchronization with the Public Cloud
            - Storage Servers
            - Application Servers
            - Database Server
    - WAN
        i. Multi-homed setup (i.e., Multiple ISPs)
        ii. SMTP Server
        iii. SaaS
            - VoIP System
            - CRM Tools
            - Email Services
            - Document Processing Tool(s)
            - Networking Services
        iv. Domain Controller
        v. IaaS, PaaS and Data Synchronization with the Private Cloud
            - Application Hosting
            - Storage Hosting
            - Database Hosting

vi. System Security Management and Monitoring
vii. Cloud Security

Requirement Details[9]**:**

LAN:

- VoIP Systems
  - This solution will be cloud-based
  - Hardware and software solutions installed on-premise will be compatible with this cloud-based VoIP System
  - Centralize control and over the cloud which offers the following solutions:
    - User Control and Access Management
    - Automatic Receptionist and Editable Voice Prompts
    - Call Analytics and Monitoring
    - Call Groups, Queuing, Redirect and Parking
  - Since the solutions will be cloud-based, any physical device will be PoE enabled
- Centralized Printer Systems
  - Network Printer(s) to be mapped to all end-user devices within the network
- Security Cameras
  - Preferred to be delivered through PoE
  - All footage will be stored on a local hard-drive device and the cloud as a backup
  - Accessible through:
    - Mobile App
    - Website
- End-Point Security / Anti-Malware Server
  - Installation of AV features to end-devices via an Anti-Malware Server to protect users from external threats in case these were undetected with the edge firewalls
- VPN Server
  - Hosted locally and is used by VPN Clients to connect to the local network through the Internet
- Intermediary Device and Device Management
  - On-premise devices should able to deliver the LAN infrastructure and be easily managed for maintenance and monitoring activities
  - This could include the following resources
    - Switches
    - Routers
    - Security Appliances
    - Other critical Data Center components

[9] Due to the limited scope of this study, it should be noted that some of these requirements will not be covered in full detail. Moreover, additional external resources will be provided for these undiscussed topics.

- LAN Optimization
    - Network Subnetting and VLANs
        - The network is to be subdivided into different networks (i.e., Public or Private LAN) to accommodate different network environments which are as follows:
            a. Production Environment
                i. Workstations
                ii. Phones
                iii. Printers
                iv. Intermediary Devices
                v. VM Instances
                vi. Storage Instances
                vii. Database Instances
            b. UAT and Dev Environments
                i. Workstations
                ii. Intermediary Devices
                iii. VM Instances
                iv. Storage Instances
                v. Database Instances
    - Network Security
        - Security appliances shall be added within the edge of the on-premise network to provide IPS, IDS, and Firewall features for the LAN
    - Device HA and Redundancy
        - Devices that are considered as core pathways in which information is being delivered has a redundant device installed such then when the primary device fails, the secondary devices automatically assumes the responsibility of the operations to be performed
        - Redundant links are also created such that it will failover to the next best path in case a particular link fails
- Server Setup
    - Storage Servers
        - This will provide a centralized storage platform which will have high data availability delivered through Storage Area Networks (SAN)
        - Provides storage capabilities to the production network resources such as:
            a. To other Servers via its hosted VM instances
            b. To workstations
    - Application Servers
        - Hosts applications critical for business operations within the production network
        - This includes applications such as:
            a. Locally created Applications
            b. Web Applications and Website Hosting Instances
            c. Mobile Applications

    - Database Servers
        - Servers that host databases needed by applications to perform business operations

WAN:

- Internet Connectivity
    - Multiple ISPs are set up such that when one ISP fails, all services can be delivered through the next ISP available
        - Services include Web Applications, Web sites, and Mobile Applications
    - A range of multiple public IP addresses will be requested and registered under the organization to provide public access to such service/application through Address Translation protocols and will be redirected using DNS Servers
- SMTP Server
    - It is used to send out a limited number of outbound emails
    - The use case for this SMTP Server are as follows:
        - Sending out emails through Website Application (i.e., front-end and back-end services)
        - Sending out emails from corporate printers
- SaaS
    - Managed externally by a SaaS provider
    - The required applications include the following:
        - VoIP System
        - CRM Tools
        - Emails
        - Document Processing Tools
        - Networking Services
- PaaS
    - External PaaS provider will provide a platform to deliver a development environment for developers to build, debug and test applications before UAT and deployment
- IaaS
    - External IaaS provider will manage the compute, storage, database and security services for this infrastructure but will offer the ability for the organization to set up their infrastructure to this IaaS environment
- Domain Controllers
    - The server will provide automatic IPv4 Address, default gateway, DNS settings, account authentication, and management to correctly identify and give access to resources across the organization’s computing system.

- DNS Server
    - External DNS Service provider gives the capability to customize the registered domain entries to provide security, name mapping services to private resources and other related services
- System Security Management and Monitoring
    - This will be used to manage cloud security services and to monitor critical parameters and resources for maintenance, monitoring and troubleshooting initiatives within the organization
- Connectivity to Community Networks
    - Delivers the connection of the organization to industry community networks needed to acquire information from the organization's clients
    - This connection will be delivered in compliance with the industry IT standards and guidelines

Cloud Solutions

The following services taken from AWS, Azure, and GCP will be used for this section of the study. These services have been taken from the services highlighted in Section 3 and were selected to satisfy the requirements for this Medium Business Model. Please do note that these selected services could be further filtered based on the business requirements. For more information regarding these selected services, please refer to the Appendix section of this documentation.

Cloud Service Provider	Basic Compute
Amazon Web Services	**EC2**; Lightsail; VMware Cloud on AWS
Microsoft Azure	**Virtual Machines**; Virtual Scale Sets
Google Cloud Platform	**Compute Engine**

Table 32 – Medium Business – Summary: Compute Services
This will be used to satisfy the compute requirement of the organization

Cloud Service Provider	Block Storage	File Storage	Object Storage	Archival Services	Disaster Recovery
Amazon Web Services	**EBS**	**EFS**	**S3**	**Glacier**	**CloudEndure**
Microsoft Azure	**Block Blob Storage**	**File Storage**	**Blob Storage**; Queue Storage; Data Lake Store	**Backup**	**Site Recovery**
Google Cloud Platform	**Persistent Disk**	**Cloud Filestore**	**Cloud Storage**	**Cloud Storage**	N/A

Table 33 – Medium Business – Summary: Storage Services
This will be used to satisfy the storage requirement of the organization

Cloud Service Provider	Virtual Private Cloud	Lease Line Services	DNS
Amazon Web Services	**VPC**	**Direct Connect**	**Router 53**
Microsoft Azure	**Virtual Network; VPN Gateway**	**Virtual Network**	**Azure DNS**
Google Cloud Platform	**Virtual Private Cloud**	**Cloud Interconnect**; Network Service Tiers	**Cloud DNS**

Table 34 – Medium Business – Summary: Networking Services
This will be used to satisfy the networking requirement of the organization

Cloud Service Provider	Relational/SQL Database	NoSQL Database
Amazon Web Services	**RDS;** Aurora; Neptune	**DynamoDB**
Microsoft Azure	**SQL Database**; Database for MySQL; Database for PostgreSQL; Server Stretch Database; Data Factory	**Cosmos DB**; Table Storage
Google Cloud Platform	**Cloud SQL**; Cloud Spanner	**Cloud Bigtable; Cloud Datastore**

Table 35 – Medium Business – Summary: Database Services
This will be used to satisfy the database requirement of the organization

Cloud Service Provider	Cloud Monitoring	Cloud Management
Amazon Web Services	**CloudWatch; CloudTrail**	**Systems Manager;** Management Console; Auto Scaling; Elastic Load Balancing
Microsoft Azure	**Monitor; Log Analytics**	Portal; **Policy; Cost Management**
Google Cloud Platform	**Stackdriver**	**Stackdriver**

Table 36 – Medium Business – Summary: Monitoring and Management Services
This will be used to monitor and manage the cloud service utilized by the organization

Cloud Service Provider	Security	Authentication and Access Management
Amazon Web Services	**GuardDuty; Macie; Shield; WAF**	**IAM; Directory Service; Organizations; Single Sign-On**
Microsoft Azure	**Security Center**	**Active Directory**; Multi-Factor Authentication
Google Cloud Platform	**Cloud DLP; Cloud Security Scanner**	**Cloud IAM; Cloud IAP**

Table 37 – Medium Business – Summary: Security and Access Management Services
This will be used to provide security and access management to the organization

CSP Services

As the general requirement, the organization needs to provide a secure and reliable network that would provide high data availability and satisfy the required data residency guidelines posted by their industry bodies. The organization will also require Business Continuity (BC) and Disaster Recovery (DR) Strategies to continue with business processes in case of a natural, technological, and man-made disaster(s).

Basic Requirements

Several computing and other technological requirements have been highlighted. This includes VoIP, Printer, and Camera Systems. For these requirements, the organization would require a cloud solution to support these requirements. However, this would still involve buying VoIP devices or headphones to support SaaS applications. Such cloud services could include namely Amazon Connect, Microsoft Business Voice, and Google Voice. There are many options for VoIP services, which are also dependent on Telecommunications Service Providers such as Telus, Shaw, and Bell. These are region-specific and can vary depending on which country and region an organization is located.

For medium businesses, Printer and Camera systems would be installed on-premise. Printers will be connected via TCP/IP, and appropriate drivers will be installed to user workstations dependent on the type of printer is being installed. Camera systems will be connected to a video recording device on-premise, with an option to transfer the files through file transfer protocols and storage solutions available within the cloud.

Another requirement highlighted was End-Point Security. For medium businesses, this will typically involve an Anti-Malware server, such as Symantec End-Point Protection Server, in which applicable licenses will be available to be assigned for users within the organization. The actual end-point security application will then be installed within end-user workstations, and all updates will be centralized and pushed from this server.

Intermediary devices must be set up to establish the LAN network. Devices required include Cisco routers, switches, access points, and relevant security appliances. The security appliances will provide on-premise security against malware, address translation functionalities, and would provide VPN access for remote users outside the organization. Appropriate network subnetting, address allocation, and VLAN assignments must be done while considering designs to implement separate network domains to support the Development, UAT (User Acceptance Testing), and Production environments. Polices will be implemented using various frameworks such as NIST, ITIL, COBIT, and ISO to provide a system and organizational security to mitigate any risks involving natural and man-made disasters.

A secure and reliable Internet connection must be obtained from Internet Service Providers (ISP – in a dual-homed configuration) for the organization to connect to the WAN network, and ultimately, access cloud services to set up the organization's Hybrid Cloud Architecture. The organization must request and reserve several IP ranges such that it can be utilized to support and host public applications and resources to serve its client base and to deliver ISP and IP connection redundancy within the organization.

Another critical resource is an SMTP server. This enables users to send marketing, or application-generated emails, which are primary drivers for performing e-mail notifications and campaigns on behalf of the organization. There are cloud solutions implementations that would provide SMTP features such as Amazon SES, Azure Plug-in Twilio SendGrid, and GCP Firebase Cloud Messaging.

Critical On-Premise Requirements

In order to support on-premise applications and services, data center design, computing system installation, and delivery must be done.

Application Servers will host all critical applications required for business operations. This could include the local Production, UAT, and Dev resources, which runs applications responsible for executing locally developed applications, web/mobile applications, and stack managers (i.e., MANO – Management and Orchestration tools) that manage and monitor other vital VM instances for the organization. The most critical resources for these devices are Core Processors and Memory. Manipulating these factors will affect the performs of the server and all the VMs hosted within the server. Such servers that can be implemented will include Dell Servers having VMWare Hypervisor configured to enable VM hosting.

Storage Servers will be implemented as a Storage Area Network and provide features that will enable computing instances within servers and workstations within the organization to allocate these virtual hard disk space locally. Redundancy features within the disk arrays, such as with RAID, while performing duplication and high data availability processes such as Striping, Mirroring, or Parity. These redundancy features will then affect the total effective hard disk space that can be utilized, which is the most critical resource for this device. Such servers that can be implemented will include NetApp FAS, which also offers cloud storage solutions and integration with the AWS, Azure, and GCP.

Database Servers will be delivered to host database instances, which are used in parallel with applications hosted within the Application Server. Maintaining Database availability is critical since this is one of the primary drivers for organizations to perform day to day business operations and to provide services to its client base efficiently. Such server that can be implemented includes Oracle Database.

Compute Replication should be performed to the redundant site(s) ahead of time so that any redundant site can easily assume the responsibility to perform the necessary compute operations for the organization. This is done by creating a copy of a compute instance from one of the servers hosting a specific VM instance and cloning it to another remote host device. In order for the organization to fully implement this Hybrid Cloud Environment that aims to provide Site Redundancy, data synchronization technologies should also be considered in order to keep up-to-date data and applications between these two sites. This is critical so that if one site fails, all processes can be easily transferred to the alternate site. Once the issues within the site that failed have been resolved, business processes will return to its normal operations (i.e., in line with an organization's Business Continuity and Disaster Recovery Procedures). Several data synchronization tools can be used for on-premise resources that are compatible with AWS, Azure, and GCP, such as Active Data Guard (for Oracle Database Servers) and SnapMirror and Cloud Sync (for NetApp Storage Servers).

Connection to Community Networks

In order to acquire critical and confidential Industry-based information (e.g., Health Care, Government, Etc.), which will be utilized within the organization, connection to Community Networks is necessary. Specific guidelines are implemented by the organization hosting the Community Network in which member organizations must align with to enable this connection. This connection involves API integrations with the public community network servers hosting authentication, security, and data transfer between a Community Network and its member(s). These edge servers will then provide the necessary connection to get and send queries from one another.

Critical Cloud Requirements

After capturing the overall information regarding the organization, consideration must be made for the most critical cloud requirements that will require Cloud Services namely CRM Tools, E-mail Services, Document Processing Tools, IaaS and PaaS deployment and computing instances which would host various services including Domain Controllers, DNS Servers, System Security Management, and Monitoring and Cloud Security. Ultimately, any integrations with third-party networks must be considered to fulfill the requirements of the industry practices needed to perform business operations within the organization.

CRM Tools (SaaS) is designed for organizations to better understand the needs and manage the interaction of the organization's client base and its potential customers. AWS, Azure, and GCP provide services for this as a plug-in from other third-party SaaS organizations. An Azure CRM service, namely Dynamics 365, is also a popular choice for systems with integrations with Microsoft. Stand-alone CRM applications, such as HubSpot, Salesforce, Zoho CRM, and LiveChat are also available, which has integration to most of these Cloud Service Providers.

E-mail service (SaaS) is a critical tool within organizations to send-out and receive messages to/from external organizations. This tool is often integrated with Calendaring and Collaboration services within an application running these services. AWS, Azure, and GCP have created solutions for these services, namely the AWS WorkMail, Microsoft Exchange, and Google Mail[10].

Document Processing Tools (SaaS) are applications that allow users to create human-readable files. The most popular tools in today's market are Microsoft Office and Google Drive Services[11].

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Productivity Service	Amazon WorkMail	Microsoft Exchange and Office	G Suite
Plan	-	Office 365 Business Premium	Business
Cost	$4 per user	$16 per user	$15.6 per user
Data Residency	US	Most Critical Applications located in Canada, with some minor services stored in the US	US
Features	Provides Email services and some Microsoft Service Integration	Includes most critical Productivity applications and some Management Features	Includes most critical Productivity applications, Security and Management Features
Dedicated Mobile Applications	None. Uses Web applications.	Yes	None. Uses Web Applications.

Table 38 – Medium Business: Productivity Services

[10] It should be noted that Microsoft Exchange and Google Mail is the most mature E-mail Services available in the today's market. Organizations will be able to leverage all the integrations available for this service to other compatible services.

[11] Together with all other productivity tools such as E-mails, Calendars and Document Processing makes up Office 365 or Microsoft Suite (i.e., Microsoft) and G Suite (i.e., Google).

Dedicated services that would enable user access and management are critical for larger organizations. Identity and Access Management (I&AM) (SaaS) is the ability of the system to provide access classification to users within the organization. However, there are also services provided by CSPs that relate not just to users but also with devices. This is done by DHCP servers, which provides appropriate device addressing information for the organization. These features comprise a Domain Controller that performs security authentication and information requests from the organization's domain. Services such as Windows Server, a product suite from Microsoft that includes features such as Active Directory, DHCP, File, and DNS services (SaaS), integrates on-premise resources to the Azure environment. Other CSP providers, such as AWS and GCP, enables integration of their platform to these features as this is a robust and proven system that that supports Windows workstations, which are the majority of end-user devices utilized within any organization. The following CSP and I&AM services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Medium Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Authentication and Access Management Service	I&AM	Active Directory	Cloud IAM
Cost	Free	Free	Free
Data Residency	US	US/CA	US/CA
Availability	99.90%	99.90%	99.95%

Table 39 – Medium Business: Authentication and Access Management Services

Computing resources (IaaS/PaaS) in the cloud will require a compute instance to host and run applications that will support the business' operations. Such computing instances can host VMs, which will then execute processes based on services configured into it. This could include web applications (i.e., public) and stand-alone applications used within the organization (i.e., private). There are other dedicated compute instances the support specific services such as web hosting, app hosting, containers, serverless architectures, development, big data analytics, batch processing, and other specialized compute requirements. Compute instances are either IaaS or PaaS offering from cloud service providers, and depending on which service is utilized based on the needs of an organization, one can select from the other. For this paper, the following IaaS Compute services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Medium Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Compute Service	EC2	Virtual Machines	Compute Engine
Cost	Customizable depending on the design	Customizable depending on the design	Customizable depending on the design
Data Residency	US/CA	US/CA	US/CA
Availability	99.99%	99.95%	99.99%

Table 40 – Medium Business: Compute Services

Storage systems (IaaS) are critical for the organization's business continuity and disaster recovery strategies. It enables the organization to continue business operations in case of natural or man-made disasters affecting the corporate environment. For Medium Businesses, Block, File, and Object storage solutions are applicable. File Storage presents information as multiple levels of files organized in folders. Block Storage divides information into arbitrary, organized equal chunks of data. Lastly, Object Storage stores data and associates it with its corresponding metadata. (Red Hat, 2020). For this organization, it will be utilizing both File and Block Storage Solutions with proper deduplication strategies for both instances in order to save storage utilization and costs. It will not be utilizing Object Storage as the computing and storage resources will be running in the same local network (i.e., either running in the public or private cloud in an active-passive setup) and will not require API storage integrations.

Archival systems (IaaS) are also part of the organization's storage systems. This solution enables organizations to store files that will be left unaccessed for long periods due to the organization's data archival guidelines in compliance with industry standards. AWS and Azure have established Disaster Recovery (DR) services (DRaaS) to solve the Business Continuity (BC) and DR requirements of an organization. The following Storage and DR Services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Medium Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Block Storage Services	EBS	Block Blob Storage	Persistent Disk
Cost	**Storage**: $0.10 per GB/Month **Snapshots**: $0.05 per GB/month **Restoration**: $0.75 per hour per AZ (min. of 1 hour is charged)	**Storage**: $0.192 per GB (first 50 TB)/month **Operations**: $0.09 per 10,000 Requests	**Storage**: $0.187 per GB/month **Operations**: Free
Data Residency	US/CA	US/CA	US/CA
Availability	99.90%	99.90%	99.95%

Table 41 – Medium Business: Block Storage Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
File Storage Service	EFS	File Storage	File Store
Cost	$0.3 per GB/month	$0.074 per GB/month	$0.2 per GB/month
Data Residency	US/CA	US/CA	US/CA
Availability	99.90%	99.99%	99.90%

Table 42 – Medium Business: File Storage Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Archival Services	Glacier	Backup (Blob)	Cloud Storage
Cost	**Storage**: $0.004 GB/month Upload: $0.05 per 1000 **Upload Requests** **Retrieval**: $0.01 per GB Data **Transfer**: $0.02 per GB	**Storage**: $6.4 (base payment up to 50 GB) + $0.0287 per GB + Blob Storage Operational Costs **Operations**: $0.09 per 10,000 Requests	**Storage**: $0.026 GB/month Operation: $0.05 per 10,000 **Operations Retrieval**: $0.01 per GB **Transfer**: $0.12 per GB
Data Residency	US/CA	US/CA	US/CA
Availability	99.99%	99.90%	99.95%

Table 43 – Medium Business: Archival Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Disaster Recovery	CloudEndure	Site Recovery	-
Cost	$0.028 per source server per hour	$32 per month per protected instance	-
Data Residency	US/CA	US/CA	-
RPO/RTO	seconds/minutes	99.90%	-

Table 44 – Medium Business: Disaster Recovery Services

Database resources (PaaS) in the cloud will run on a pre-set database operating system that will host critical instances that stores information and receives/replies to queries associated with any operations performed in the application. There are two (2) major structures for databases. These are Relational Databases (SQL) and Non-relational Databases (NoSQL). SQL is structured databases that rely on indexes and the relations of tables and the relation of multiple tables (entities/objects), columns (data sets) and rows (records). As the approach for SQL is more rigid, NoSQL offers greater flexibility and adaptability with the applications that best work with unstructured data models (Williams, 2019). For this organization, it will be utilizing both types of Database solutions. For its transactional process, it will be utilizing SQL Database while on NoSQL Database for its reporting and analytics requirements.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Relational/SQL Database Services	AWS RDS - Oracle	SQL Database	Cloud SQL
Cost	Customizable depending on the design	Customizable depending on the design	Customizable depending on the design
Data Residency	US/CA	US/CA	US/CA
Availability	99.95%	99.99%	99.95%

Table 45 – Medium Business: Relational Database Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Non-Relational/NoSQL Database Services	Dynamo DB	Cosmos DB	Cloud Bigtable
Cost	**Writes**: $0.00065 per WCU **Reads**: $0.00013 per RCU **Storage**: $0.25 per GB after 25GB **Transfer**: starting from $0.09 with 10TB/month	**Requests**: $0.016 per 100 RU **Storage**: $0.32 per GB/month **Transfer**: $0.0103 100 RU/hour	**Instance**: $0.72 per hour/node **Storage**: $0.19 per GB/month **Transfer** $0.12 /GB for a 1TB limit monthly usage
Data Residency	US/CA	US/CA	US/CA
Availability	99.99%	99.99%	99.99%

Table 46 – Medium Business: Non-Relational Database Services

In order to have real-time information regarding all the cloud resources utilized by the organization, Cloud Monitoring and Management services should also be considered. This is useful for monitoring the cloud computing systems' health, determining diagnostic information, and troubleshooting should there be any issues within these resources. The following Cloud Monitoring and Management services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Medium Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Cloud Monitoring Services	CloudWatch; CloudTrail	Monitor; Log Analytics	Stackdriver
Cost	**CloudWatch**: $0.3 per month **CloudTrail**: $2.1 per 100,000 events	$2.76 per GB after 5GB	**Logging**: $0.5/GiB Data **Monitoring**: $0.151/MiB **API Monitoring**: $0.01/1,000 requests
Data Residency	US/CA	US/CA	US/CA
Availability	99.9%, 99.9%	99.90%	99.95%

Table 47 – Medium Business: Cloud Monitoring Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Cloud Management Services	Systems Manager;	Policy; Cost Management	Stackdriver
Cost	**OpsItems**: $2.97 per 1000 issues **Requests**: $0.039 per 1,000 requests	Free	**Logging**: $0.5/GiB Data **Monitoring**: $0.151/MiB **API Monitoring**: $0.01/1,000 requests
Data Residency	US/CA	US/CA	US/CA
Availability	99.90%	No SLA	99.95%

Table 48 – Medium Business: Cloud Management Services

Networking resources (IaaS/PaaS/SaaS) are essential services that will provide networking functionalities similar to how intermediary devices (such as routers, switches, and other networking appliances) perform processes for the organization. These allow flexibility by utilizing such networking services without the users getting to be familiar with a specific device model such as Cisco, Juniper, and Alcatel. Aside from connecting local and remote resources through routing and switching, these also provide other networking functionalities such as DHCP, DNS, Address Translation, and VPN services. Relating to networking services, compute instances such as Windows Server can also provide services that include DHCP and DNS services. DNS services can also be provided by the organization's ISP upon request and can be accessed from third-party DNS service providers such as Cloudflare. For this paper, the following Networking services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Medium Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
DNS Services	Route 53	Azure DNS	Cloud DNS
Cost	**DNS Server**: $0.5 per hosted zone/month **Queries**: $0.4 per 1st billion req/month	**DNS Server**: $0.64 per zone/month for first 25 **Queries**: $0.512 per 1st million req/month	**DNS Server**: $0.2 per zone/month for first 25 **Queries**: $0.4 per million req/month for the first billion req
Data Residency	US/CA	US/CA	US/CA
Availability	100.00%	100.00%	100.00%

Table 49 – Medium Business: DNS Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Virtual Private Cloud Services	VPC	Virtual Network; VPN Gateway	Virtual Private Cloud; Cloud NAT
Cost	**Site to Site**: $0.05 per connection/hour **Client VPN**: $0.15 per connection/subnet/hour **NAT Gateway**: $0.045 per NAT GW/hour **NAT Processing**: $0.045 per GB processed	**[Virtual Network]** **VNET Peering**: Zone Dependent **[VPN Gateway]** **Site to Site**: $0.02 per connection/hour after first 10 **Client VPN**: $0.013 per connection/hour after first 128 **VPN Gateway**: $4.672/hr **Data Transfer**: $0.112/GB	**[Virtual Private Cloud]** **VPN Connection**: $0.05 per tunnel/hr **Data Transfer**: $0.01/GB **[Cloud NAT]** **Instance**: $0.044/hr **NAT Processing**: $0.045/GB processed
Data Residency	US/CA	US/CA	US/CA
Availability	99.90%	99.95%, 99.95%	99.95%, 99.9%

Table 50 – Medium Business: Virtual Private Cloud Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Lease Line Services	Direct Connect	ExpressRoute	Cloud Interconnect
Cost	**Connections**: $0.3 per GB/hour or $2,190 at 10GB/month **Data Rate**: $0.02 per GB	**Connections**: $4,352 at 10GB per month **Data Rate**: $0.032/GB	**Connection**: $1,700 at 10GB per month **Data Rates**: $0.02/GB
Data Residency	US/CA	US/CA	US/CA
Availability	99.90%	99.95%	99.99%

Table 51 – Medium Business: Leased Line Services

Security resources (SaaS) in the cloud provides the organization with high-performance security and flexibility to select which security features and critical resources will be protected. Security resources in the cloud help with Advanced Threat Protection, Risk Mitigation, and Vulnerability Identification. Ultimately, the fundamental purpose of these services is to inspect data coming in and out of the system and classify them according to risk to protect the data of the organization and continue normal business operations. For this paper, the following Security services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Medium Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Security Services	GuardDuty; Macie; Shield; WAF	Security Center	Cloud DLP; Cloud Security Scanner
Cost	**[GuardDuty]** **VPC Log/DNS Analysis**: $1.00 per first 500GB/month **CloudTrail Event Analysis**: $4.00 per 1million events **[Macie]** **Content Classification**: $5.00 per GB after free 1GB **Cloud Trail Event Processing**: $4.00 per 1million events after free 100,000 events **[Shield]** **Data Transfer**: $0.05 for first 100TB per service protected (which includes CloudFront, ELB, Elastic IP, and Global Accelerator) **[WAF] Web ACL**: $5.00 per entry/month Rule: $1.00 per entry/month **Requests**: $0.6 per 1million requests	**[Protected Resources]** **Virtual Machine**: $0.026 per Server/Hr **Database**: $0.027 per Server/Hour **Storage**: $0.026 per 10k transactions	**[Cloud DLP]** **Storage**: $1.00 per GB for up to 50TB **Content Inspection**: $3.00/GB up to 1TB **Content Transformation**: $2.00/GB up to 1TB **[Cloud Security Scanner]** Free
Data Residency	[All] US/CA, [Macie] US	US/CA	US/CA
Availability	[GuardDuty and Macie] 99.9%, [Shield] 100%, [WAF] 99.95%	99.90%	No SLA

Table 52 – Medium Business: Security Services

Analysis

Based on this medium business model, the end goal is to transfer and host all internal company applications, data, and other critical resources into the cloud. These requirements are motivated by the limitation of the organization to move from one office location to another. Currently, only on-premise LAN workstations have access to this, but by streamlining the business and its computing system, it will improve the user's flexibility to utilize, managed, and perform day-to-day business operations through the Internet. As there are limited IT staff and technology experts within the organization, it will mostly utilize third-party support and external support for on-premise and cloud service instances.

For this model, an End-Device LAN, On-Prem Server LAN (i.e., Redundant Site), VPN LAN, Wireless LAN, and Cloud Services (i.e., Primary Site) would comprise this Hybrid Cloud Architecture. Since there are more complexity and sensitivity with the device and services hosted within this Hybrid Network, proper network segregation is necessary, which is performed by on-premise and cloud networking and security services. Both sites will have compute, storage, database, management, monitoring, and disaster recovery services in order to maintain site synchronization (i.e., through an active-passive configuration) and data protection for all of its application end-points.

End-Device LAN enables users within the organization's office to access all corporate computing resources needed to perform day-to-day business processes. By enabling a web-based application stack, this End-Device LAN will enable users to access the required application necessary to perform these tasks remotely.

On-Prem LAN serves as the redundant site that will host and continuously sync information from the primary site such that if the primary (i.e., the external Cloud services utilized by the organization) fails, this redundant site will assume all processes until all issues are resolved. This will be delivered through disaster recovery features within the CSP that the organization will utilize. It should be noted that the networking rules associated with the Community network must be considered during these scenarios.

VPN LAN delivers a network segment that allows remote users to connect to the On-Prem LAN/Cloud Services and access various computing resources. It is also needed to establish a secure site-to-site connection between these two (2) remote locations (again, with proper consideration for the connection between any of these sites to the Community network). Proper permissions and security roles must be made to limit and mitigate risks associated with cybersecurity threats.

Wireless LAN will be utilized within the organization to access any content within the Internet. As this is a discrete domain, there is some separation between devices within the organization's corporate LANs, so any issues from one LAN will not affect the other.

The organization will utilize various Cloud Services, including various IaaS, PaaS, and SaaS offerings associated with Compute, Storage, Database, and Networking services

as well as productivity tools, I&AM, data synchronization compatible with on-premise devices, disaster recovery, security, and cloud service monitoring and management.

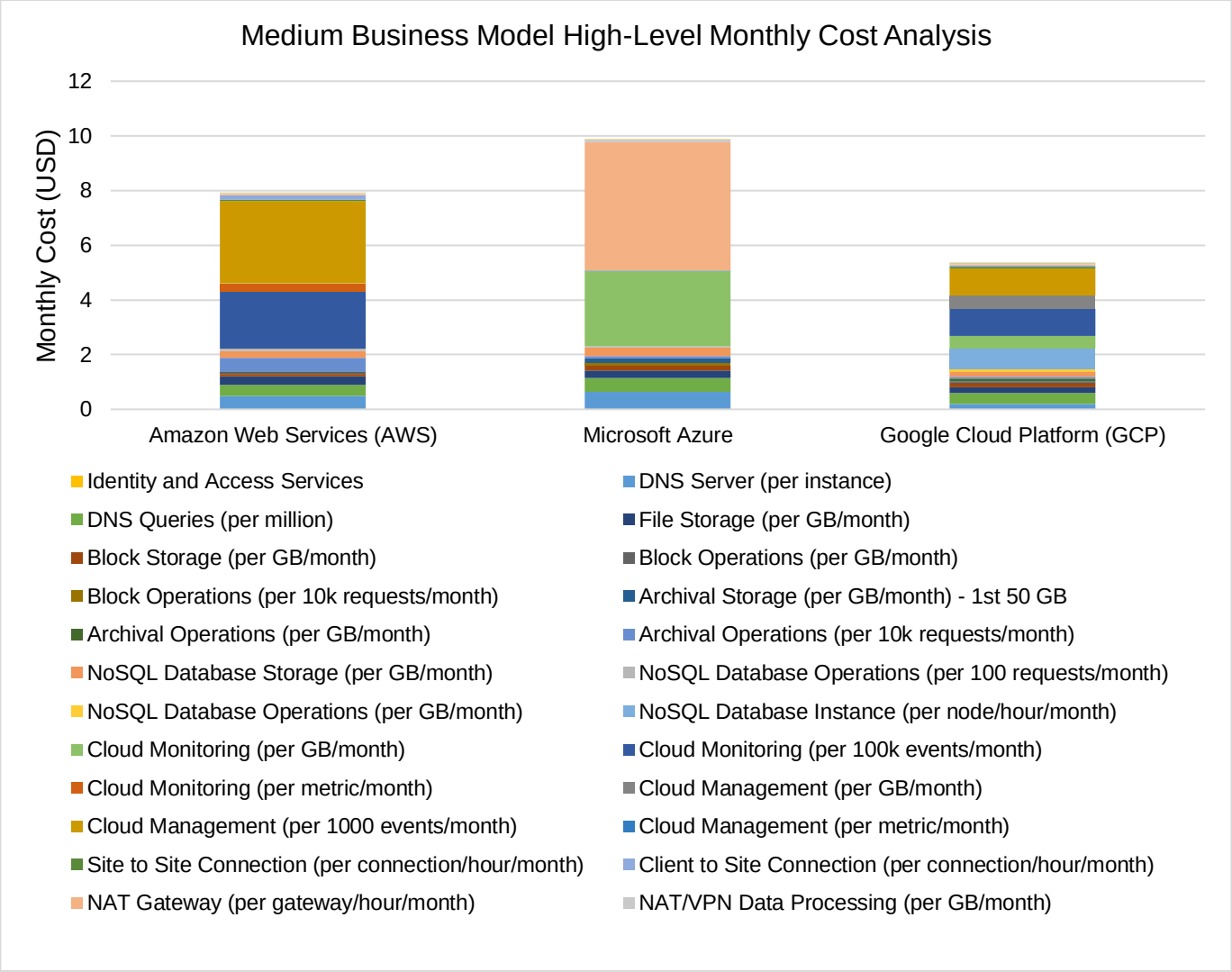

Figure 32 - Medium Business Cost Analysis

For this analysis, the following cost information has been removed to primarily focus on other critical services to be utilized from these CSPs to implement the requirements of this organization[12]:

a. Productivity tools;
b. Security services – For this documentation, AWS has more basic security features relative to other, such that it will effectively reflect higher costs;
c. Disaster Recovery Services – For this cost analysis, all services are incurred every month. However, DR services are incurred on an hourly basis;

[12] For the pricing information of these services, please see the CSP Services section of this Medium Business Modeling and Scenario.

d. Leased Line Connection – For this cost analysis, lines are rated at 10GB/month. However, its price point is above $1,000.

Based on the graph relating to the organization's monthly cost, it could be seen from this high-level cost analysis that if these cloud services are compared, Azure has the highest cost for the organization's requirement implementation. This is primarily brought by the following factors:

- The services selected for this study to deliver its requirements[13];
- The pricing of the services at the time of writing the documentation;
- The cost of utilizing Networking Gateway Services (i.e., highest cost contributor for Azure); and,
- The cost of utilizing Cloud Management and Monitoring Services (i.e., highest cost contributor for all CSPs).

For this high-level cost analysis, preference could be given for both AWS and Microsoft Azure to implement their requirements. Unfortunately, GCP will not be considered since it does not have a dedicated disaster recovery service, which if primary importance to the organization. Location, for which the service stores its information to deliver its actual services, should also be considered for these services. Based on the provided information above, all services considered from these CSPs are hosted in Canada, satisfying the data residency requirements of the organization.

It should be noted that there would be four (4) main requirements for the organization. This will involve hosting all their services in the cloud through the local region in one availability zone (including security, management, and monitoring) in compliance with industry standards, establish a disaster recovery strategy to continue its services by creating site redundancy, selecting the most appropriate productivity tools for the organization and providing proper access and permission roles for these resources. In order to harness the best benefits of both cloud systems, we can consider selecting two (2) CSPs to implement service hosting, security, management, monitoring, and disaster recovery strategies (1), and domain access and productivity tools (1).

By splitting these requirements into two (2) services providers, the organization will be able to sustain and continue business operations if ever CSPs fail. This also provides a layer of management in terms of associating all computing systems to one CSP and all productivity and access services to another CSP.

Based on all the information discussed, the organization will be utilizing AWS for its major computing system requirements and Azure for productivity and access services. Primarily, this selection is motivated due to the robust services available between these CSPs regarding disaster recovery. The choice was also motivated by some integrations with data synchronization features of AWS and Azure as they enable compatibility with the organization`s on-premise devices. Moreover, the robustness of AWS services and

[13] It should be noted that services selected are ranging from Standard and Premium services. Most services also have added capabilities which will incur additional costs. For this study, most services selected utilized Standard Features. All prices denoted are in USD.

the Microsoft suite of services for end-user workstations, productivity tools, and access management are also part of this selection. For cloud services that will be used by the organization, it is offered using a pay-as-you-go model, such that no complex licensing processes must be made, which aids with managing all the services and related subscriptions to such services. However, this is different for some on-premise services such that proper licensing rules and auditing must be initiated to comply with that device vendor's licensing standards and related terms of agreements.

It should be noted that not the best services must be used in a hybrid cloud architecture implementation as there are also several factors outside of the scope of this study that affects the selection of cloud services in any organization. Appropriate frameworks, such as the combined AWS and Microsoft architecture framework can be used to streamline further and enhance the efficiency of the operations going forward.

Large Business Model

This section provides a high-level discussion regarding all business and computing requirements for a Large Business Organization. The paper aims to show an all-purpose template to capture all factors relevant within the organization and to ultimately utilize this information to design and deploy its Hybrid Cloud Architecture.

Overview

Name: Garden Party
Industry: South East Asia Flower Farming and Distribution
Location: Multi-national – South East Asia (Asia Pacific - i.e., Philippines, Indonesia, Thailand, and Malaysia)
End Users: ~700
Major Departments: 12
Divisions: 60

To align with standards established by Asia Pacific countries through APEC (Asia-Pacific Economic Cooperation), the organization, as an organizational standard, will adhere to guidelines related to the APEC Privacy Framework (i.e., similar to the European Union's GDPR policy)[14]. These efforts will ensure that the organization will comply and align itself with policies across this economic region with regards to delivering its business requirements.

The organization has bought several remote business units (i.e., office branches and distribution centers) between several regions in the Asia Pacific, particularly in the areas of the Philippines, Indonesia, Thailand, and Malaysia. The organization aims to connect all these different locations to its corporate network so it can acquire vital information necessary to run various business processes and continue delivering its services to its internal users and clients. From these remote locations, production and consumer units (i.e., individual local units who processed the organization's products), which could either be part or external to the organization, require access to some critical information relevant for their use. To summarize the high-level network requirement, the organization requires:

1. Product Output Network (Community Network)
    - Access is for product consumers (i.e., commercial retailers)
    - Provide information regarding product yields
    - Viewing privilege is location/division/department dependent
2. Product Input Network (Community Network)
    - Access is for product producers (i.e., individual producer units)
    - Provide information regarding product sales
    - Viewing privilege is location/division/department dependent

[14] Please do note that this framework alignment will not be discussed in full detail for this documentation.

3. Corporate Network
    - Access is for internal employees (i.e., remote office locations)
    - Take information from Product Input/Output Network, perform data analytics and other business performance tests.

There are three (3) key locations for the organization which should have high latency, high data availability, and secure connectivity.

4. Local HQ
    - Connects all local producers/consumers within the region
    - Located in Manila, Philippines
5. International Gateway HQ
    - Connects all local producers/consumers within Thailand, Malaysia, and Indonesia
    - Located in Kuala Lumpur, Malaysia
6. Trans-National Shipment Site
    - Connects shipment between the Philippines and the rest of the SEA region
    - Located in the Philippines and Indonesia

Each branch location will have a similar network implementation, which will serve as a template for all company-internal office units. The organization will migrate to a Hybrid Cloud Architecture motivated by the Total Cost of Ownership (TCO) analysis performed between maintaining an on-premise solution and migrating all services to the cloud. This migration will enable the organization to deliver services such that:

1. Most of the organization's legacy devices within the organization will be placed out of commission or will all be transferred into the cloud. This migration includes legacy Compute, Storage, Database, Network, and Security services.
2. On-premise solutions will still be in place to continue with regular business operations but must be compatible with CSP services. This will aid with data and application synchronization between these multiple locations.
3. Primary applications, storage, and database environments used by the organization will primarily be hosted on the cloud. Multiple instances of these applications will be made across the Asia Pacific region (specifically on HQ locations) to provide redundancy. To fully ensure this, various CSP providers will be utilized across the platform and an on-premise back-up stored within the organization's HQs will be established.
4. To optimize its storage and database environments, proper consideration of which storage and database solution and deduplication strategies shall be selected.
5. The cloud network and security environment will be optimized by availing other SaaS solutions to streamline business processes.

It should be noted that the organization will have no limitation with cost and prioritizes service availability and security above all else.

Topology

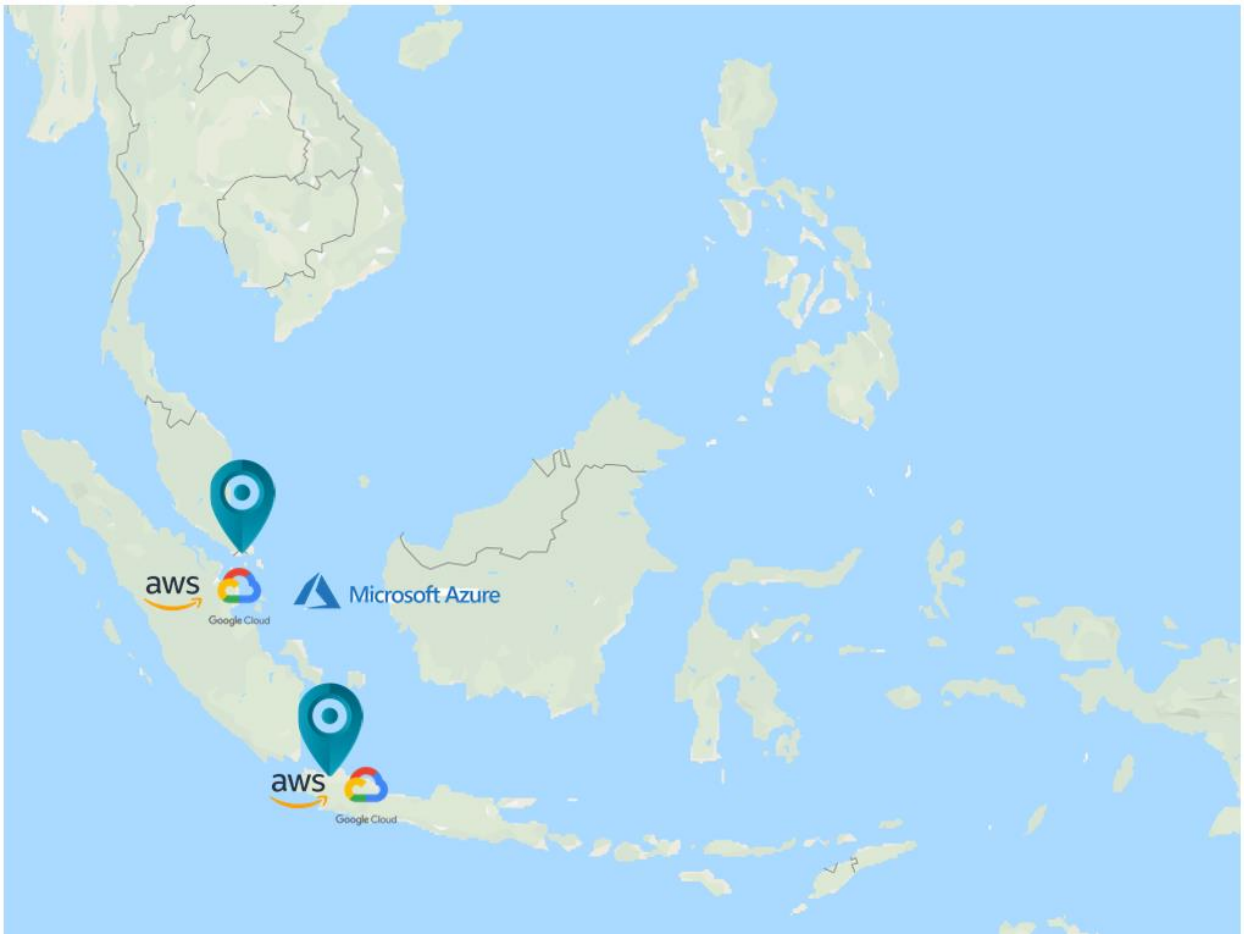

Figure 33 – CSP Regions in the Asia Pacific
(South East Asia – Singapore and Indonesia)

Figure 34 – Organizational Sites and Link Connections

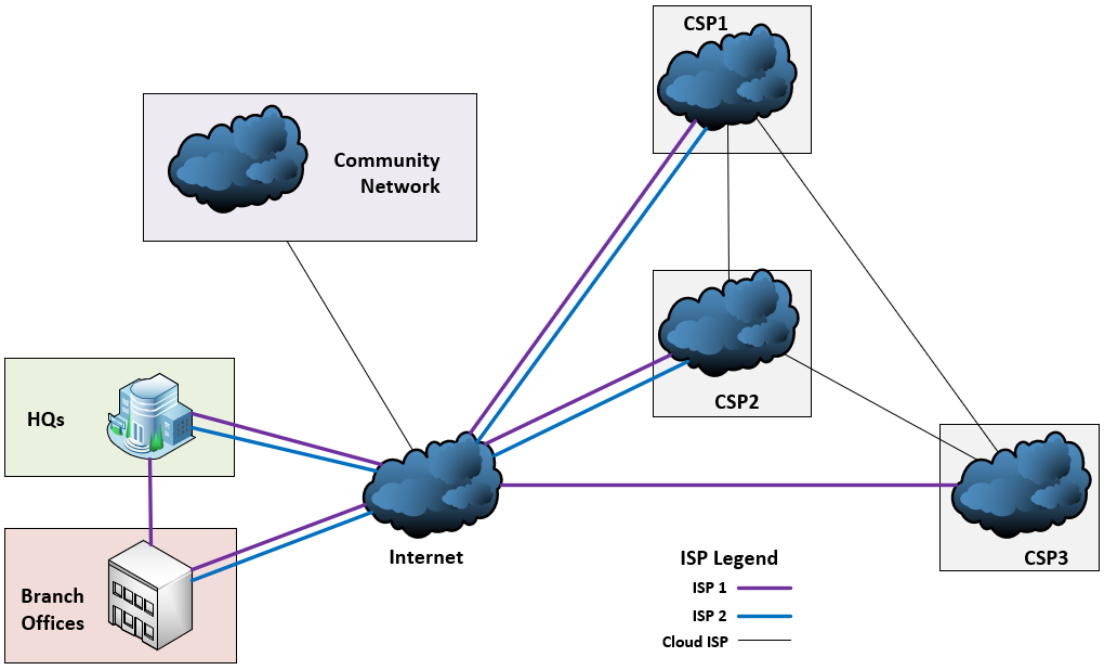

Figure 35 – High-Level Large Business Network Topology

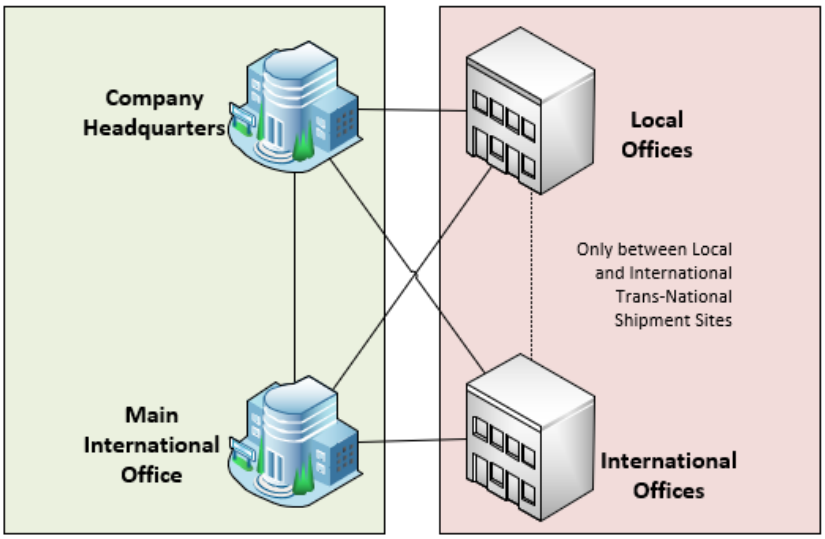

Figure 36 – Connectivity between HQs and Branch Offices

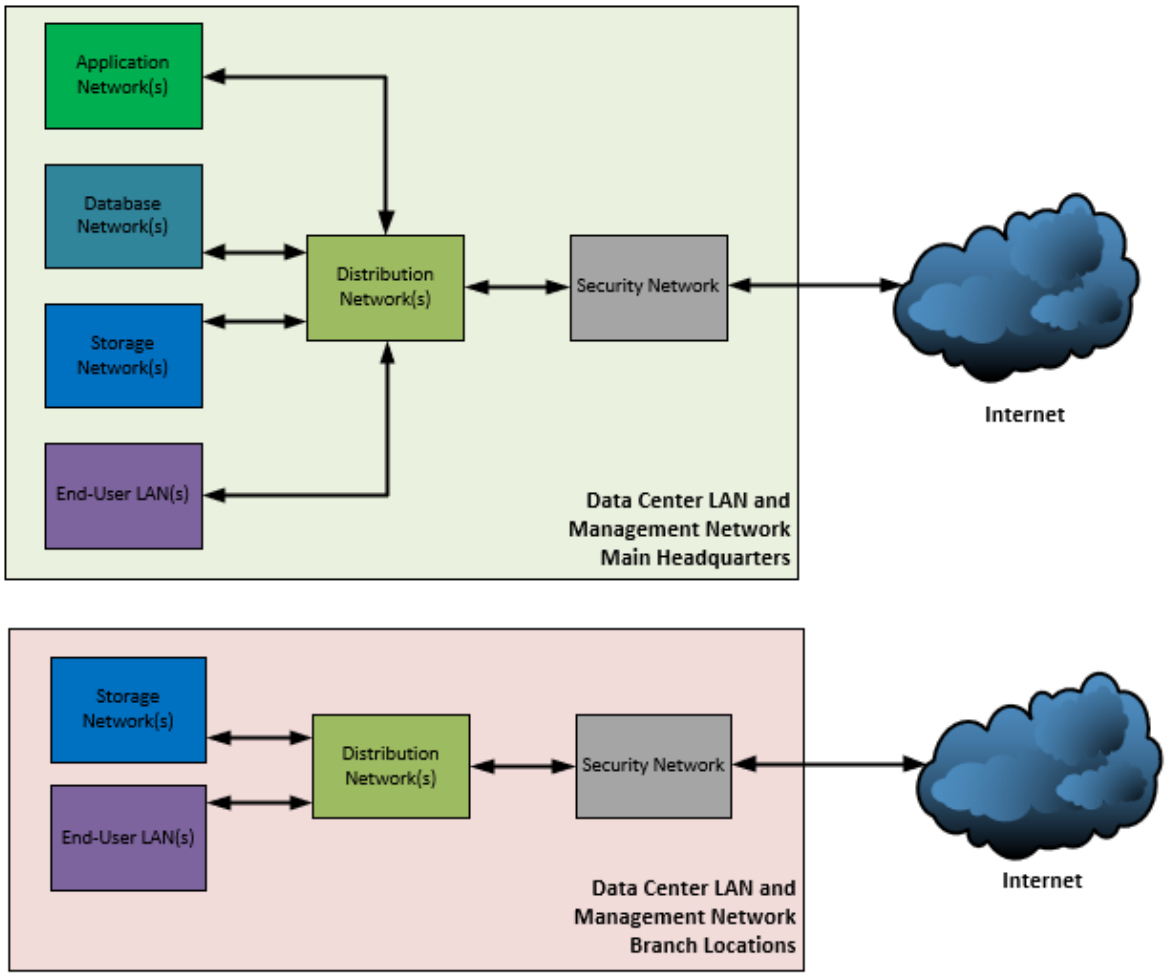

Figure 37 – Medium-Level HQ and Branch Office Network Infrastructure Topology

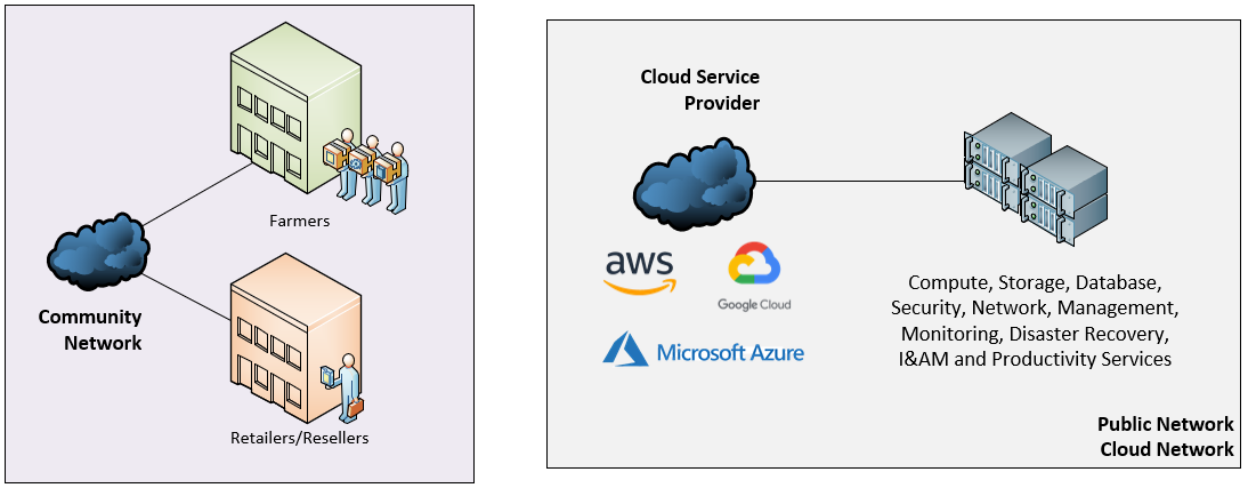

Figure 38 – Medium-Level Community and CSP Network Components/Topologies

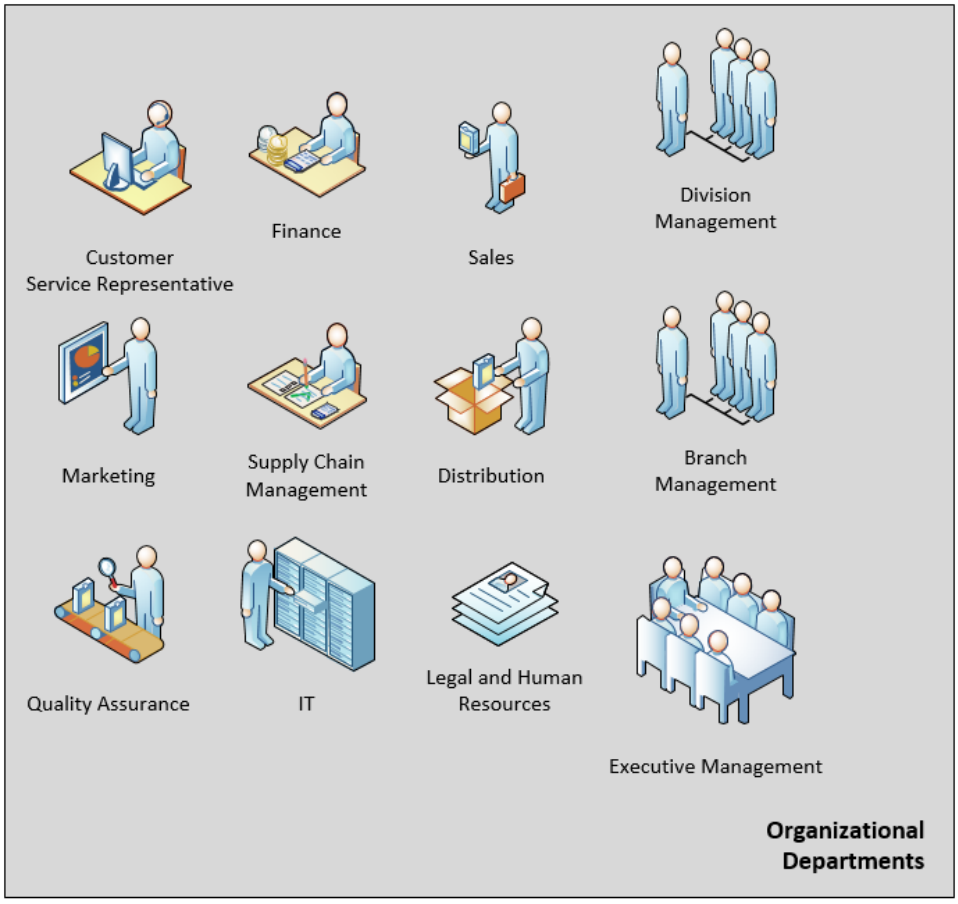

Figure 39 – Organization's Business Units within the HQ and Branch Office Locations

Requirements

Summary Requirements:

The summarized requirements for the organization are as follows:

a. Data residency policies are not strictly required for this organization.
b. The requirements will have no project cost restrictions and will utilize either on-demand and dedicated on-premise and cloud services based on the business needs
a. Equip the organization with real-time, low data latency requirements, high data availability, site, device and link redundancy, and disaster recovery features
c. Secure the connection between these multiple associated locations
d. Provide public access to external stakeholders by providing content delivery through hosting of a community network
e. Adopt and comply with the APEC Privacy Framework Compliancy
f. The organization will utilize advanced services such as:
    - IoT
    - Fog Computing
    - AI/ML
    - Data Lakes/Big Analytics
g. Create a LAN and WAN networking template for multiple branch locations while considering:
    - On-premise Setup (Private Cloud)
    - Cloud Service Setup (Public Cloud)
h. Setup cloud data synchronization between the organization`s Private and the Public Cloud environments
i. Utilize available services to migrate a legacy application to the public cloud
j. LAN and WAN Networking
    - LAN
        i. VoIP Systems
        ii. Printer Systems
        iii. Security Cameras
        iv. End-Point Security/Anti-Malware Server
        v. Intermediary Devices Management
        vi. VPN Server
        vii. LAN Optimization
            - Network Subnetting and VLANs
            - Private and Public LANs
            - Separate Network Environments
                - Production
                - UAT
                - Development
            - Network Security
        viii. Server Setup
            - Storage Servers
            - Application Servers
            - Database Servers

- WAN
  i. Multi-homed setup (i.e., Multiple ISPs)
  ii. SMTP Server
  iii. SaaS
    - VoIP System
    - CRM Tools
    - Email Services
    - Document Processing Tool(s)
    - Networking Services
  iv. Domain Controller
  v. IaaS/PaaS
    - Application Hosting
    - Storage Hosting
    - Database Hosting
  vi. System Security Management and Monitoring
  vii. Cloud Security

Requirement Details[15]:

LAN:

- Internet Connectivity
  - Multiple ISPs are set up such that when one ISP fails, all services can be delivered through the next ISP available
    - Services include Web Applications, Web sites, and Mobile Applications
  - A range of multiple public IP addresses will be requested and registered under the organization to provide public access to such service/application through Address Translation protocols and will be redirected using DNS Servers
- VoIP Systems
  - This solution will be cloud-based
  - Hardware and software solutions installed on-premise will be compatible with this cloud-based VoIP System
  - Centralize control and over the cloud which offers the following solutions:
    - User Control and Access Management
    - Automatic Receptionist and Editable Voice Prompts
    - Call Analytics and Monitoring
    - Call Groups, Queuing, Redirect and Parking
  - Since the solutions will be cloud-based, any physical device will be PoE enabled.

[15] Due to the limited scope of this study, it should be noted that some of these requirements will not be covered in full detail. Moreover, additional external resources will be provided for these undiscussed topics.

- Centralized Printer Systems
    - Network Printer to be mapped to all end-user devices within the network
- Security Cameras
    - Preferred to be delivered through PoE
    - Accessible through:
        - Mobile App
        - Website
- End-Point Security / Anti-Malware Server
    - Installation of AV features to end-devices via an Anti-Malware Server to protect users from external threats in case these were not detected with the edge firewalls
- VPN Server
    - Hosted locally and is used by VPN Clients to connect to the local network through the Internet
- Intermediary Device and Device Management
    - On-premise devices should able to deliver the LAN infrastructure and be easily managed for maintenance and monitoring activities
    - This could include the following resources
        - Switches
        - Routers
        - Security Appliances
        - Other critical Data Center components
- LAN Optimization
    - Network Subnetting and VLANs
        - The network is to be subdivided into different networks (i.e., Public or Private LAN) to accommodate different environments, namely:
            a. Production Environment
                i. Workstations
                ii. Phones
                iii. Printers
                iv. Intermediary Devices
                v. VM Instances
                vi. Storage Instances
                vii. Database Instances
            b. UAT and Dev Environments
                i. Workstations
                ii. Intermediary Devices
                iii. VM Instances
                iv. Storage Instances
                v. Database Instances
    - Network Security
        - Security appliances shall be added within the edge of the on-premise network to provide IPS, IDS, and Firewall features for the LAN

- Site, device and link redundancy
  - Enterprise network resources that are running critical resources will have multiple redundancy sites in-line the organization`s business continuity and disaster recovery initiatives
  - Devices that are considered as core pathways in which information is being delivered should have a redundant device installed such then when the primary device fails, the secondary devices automatically assumes the responsibility of the operations to be performed
  - Redundant links are also created such that it will failover to the next best path in case a particular link fails

- Server Setup
  - Storage Servers
    - This will provide a centralized storage platform which will have high data availability delivered through Storage Area Networks (SAN)
    - Provides storage capabilities to the production network resources to the following:
      a. To other servers via its hosted VM instances
      b. To workstations
  - Application Servers
    - Hosts applications critical for business operations within the production network
    - This includes services such as:
      c. Locally created applications
      d. Web Applications and Website Hosting Instances
      e. Mobile Applications
  - Database Servers
    - Servers that host databases needed by applications to perform business operations

WAN:

- Internet Connectivity
    - Multiple ISPs are set up such that when one ISP fails, all services can be delivered through the next ISP available
        - Services include Web Applications, Web sites, and Mobile Applications
    - A range of multiple public IP addresses will be requested and registered under the organization to provide public access to such applications through address translation protocols and will be redirected using DNS Servers
    - This Internet connection must be dedicated to the headquarter office locations and business class for other branch locations in a dual-homed configuration
- SMTP Server
    - It is used to send out a limited number of outbound emails
    - The use case for this SMTP Server are as follows:
        - Sending out emails through Website Application (i.e., front-end and back-end services)
        - Sending out emails from corporate printers
- SaaS
    - Managed externally by a SaaS provider
    - The required applications include the following:
        - VoIP System
        - CRM Tools
        - Emails
        - Document Processing Tools
        - Networking Services
- PaaS
    - External PaaS provider will provide a platform to deliver a development environment for developers to build, debug and test applications before UAT and deployment
- IaaS
    - External IaaS provider will manage the compute, storage, database and security services for this infrastructure but will offer the ability for the organization to set up their infrastructure to this IaaS environment
- Domain Controllers
    - Server will provide automatic IPv4 Address, default gateway, DNS settings, account authentication, and management to correctly identify and give access to resources across the organization’s computing system.
- DNS Server
    - External DNS Service provider gives the capability to customize the registered domain entries to provide security, name mapping services to private resources and other related services

- System Security Management and Monitoring
    - This will be used to manage cloud security services and to monitor critical parameters and resources for maintenance, monitoring and troubleshooting initiatives within the organization
- Content Delivery via Community Network
    - Delivers a community network that hosts content delivery features needed by the organization's clients to acquire business-related information
    - This connection will be provided in compliance with the industry IT standards and guidelines
- Migration
    - Private Cloud to Public Cloud Migration
        - Private-to-Public Cloud Migration is the shift from utilizing an on-premise cloud environment to a third-party cloud service provider (Rouse M. , 2018)
    - Public Cloud to Public Cloud Migration
        - When an organization has been using a third-party cloud service provider and want to transition to another cloud provider, Cloud-to-Cloud Migration must then be considered (Rouse M. , 2018)
    - Public Cloud to Private Cloud Migration
        - Uncloud, Declouding, or Reverse Cloud Migration is the shift from utilizing a third-party cloud service provider to an on-premise cloud solution (Rouse M. , 2018)

Cloud Solutions

The following services taken from AWS, Azure, and GCP will be used for this section of the study. These services have been taken from the services highlighted in Section 3 and were selected to satisfy the requirements for this Large Business Model. Please do note that these selected services could be further filtered based on the business requirements. For more information regarding these selected services, please refer to the Appendix section of this documentation.

Cloud Service Provider	Basic Compute	Containers	App Hosting
Amazon Web Services	**EC2**; Lightsail; VMware Cloud on AWS	ECS; EKS; ECR; Fargate	Elastic Beanstalk
Microsoft Azure	**Virtual Machines**; Virtual Scale Sets	AKS; Container Instances	App Service; Service Fabric; Cloud Services
Google Cloud Platform	**Compute Engine**	Kubernetes Engine; Knative	App Engine

Table 53 – Large Business – Summary: Compute Services
This will be used to satisfy the compute requirement of the organization

Cloud Service Provider	Block Storage	File Storage	Object Storage	Archival Services	Disaster Recovery
Amazon Web Services	**EBS**	**EFS**	**S3**	**Glacier**	**CloudEndure**
Microsoft Azure	**Block Blob Storage**	**File Storage**	**Blob Storage**; Queue Storage; Data Lake Store	**Backup**	**Site Recovery**
Google Cloud Platform	**Persistent Disk**	**Cloud Filestore**	**Cloud Storage**	**Cloud Storage**	N/A

Table 54 – Large Business – Summary: Storage Services
This will be used to satisfy the storage requirement of the organization

Cloud Service Provider	Virtual Private Cloud	Lease Line Services	Content Delivery	DNS
Amazon Web Services	**VPC**	**Direct Connect**	**CloudFront**	**Router 53**
Microsoft Azure	**Virtual Network; VPN Gateway**	**Virtual Network**	**CDN**	**Azure DNS**
Google Cloud Platform	**Virtual Private Cloud**	**Cloud Interconnect**; Network Service Tiers	**Cloud CDN**	**Cloud DNS**

Table 55 – Large Business – Summary: Networking Services
This will be used to satisfy the networking requirement of the organization

Cloud Service Provider	Relational/SQL Database	NoSQL Database
Amazon Web Services	**RDS;** Aurora; Neptune	**DynamoDB**
Microsoft Azure	**SQL Database**; Database for MySQL; Database for PostgreSQL; Server Stretch Database; Data Factory	**Cosmos DB**; Table Storage
Google Cloud Platform	**Cloud SQL**; Cloud Spanner	**Cloud Bigtable; Cloud Datastore**

Table 56 – Large Business – Summary: Relational Database Services
This will be used to satisfy the database requirement of the organization

Cloud Service Provider	Cloud Monitoring	Cloud Management
Amazon Web Services	**CloudWatch; CloudTrail**	**Systems Manager; Management Console; Auto Scaling; Elastic Load Balancing**
Microsoft Azure	**Monitor; Log Analytics**	Portal; **Policy; Cost Management**
Google Cloud Platform	**Stackdriver**	**Stackdriver**

Table 57 – Large Business – Summary: Non-Relational Database Services
This will be used to monitor and manage the cloud service utilized by the organization

Cloud Service Provider	Security	Authentication and Access Management
Amazon Web Services	**GuardDuty; Macie; Shield; WAF**	**IAM; Directory Service; Organizations; Single Sign-On**
Microsoft Azure	**Security Center**	**Active Directory**; Multi-Factor Authentication
Google Cloud Platform	**Cloud DLP; Cloud Security Scanner**	**Cloud IAM; Cloud IAP**

Table 58 – Large Business – Summary: Security and Access Management Services
This will be used to provide security and access management to the organization

Cloud Service Provider	Migration
Amazon Web Services	**AWS Database Migration; AWS Migration Hub; AWS Server Migration Service; AWS Snowball; AWS Snowball Edge; AWS Snowmobile**
Microsoft Azure	**Azure Migrate; Azure Site Recovery; Azure Database Migration Services; Data Box**
Google Cloud Platform	**Transfer Appliance; Transfer Service**

Table 59 – Large Business – Summary: Migration Services
This will be used to satisfy the migration requirements of the organization

Cloud Service Provider	Big Data Analytics
Amazon Web Services	Athena; EMR; Kinesis; Redshift
Microsoft Azure	HDInsight; Stream Analytics; Data Lake Analytics; Analysis Services
Google Cloud Platform	Cloud Dataflow; Cloud Dataproc

Table 60 – Large Business – Summary: Data Analytics Services
This will not be discussed in full detail for this documentation

Cloud Service Provider	Machine Learning	Cognitive Services	IoT	3rd Party Software and Services	Training	Support
Amazon Web Services	SageMaker; AML; Apache MXNet on AWS; TensorFlow on AWS	Comprehend; Lex; Polly; Rekognition; Translate; Transcribe	IoT Core	Marketplace	Training and Certification	Support
Microsoft Azure	Machine Learning	Cognitive Services	IoT Hub; IoT Edge	Marketplace	Training	Support
Google Cloud Platform	Cloud Machine Learning Engine	Cloud Natural Language; Cloud Speech API; Cloud Translation API; Cloud Video Intelligence	Cloud IoT Core	Cloud Launcher; Partner Directory	Training Programs	Support

Table 61 – Large Business – Summary: Other Services
This will not be discussed on full detail for this documentation

CSP Services[16]

As the organization will have multiple locations across the Asia Pacific region which needs to be associated with one another, the organization needs to provide a secure and reliable network that would give real-time high data availability with low latency and multiple service redundancies across its on-premise and cloud environments. To standardize the process within the organization with regards to technology and data protection policies, it will align its standards with the APEC Privacy Framework (i.e., synonymous with EU's GDPR). Finally, the organization will also require Business Continuity (BC), Disaster Recovery (DR), Data Synchronization, and Migration Strategies to continue with business processes in case of a natural, technological, and man-made disaster(s).

Basic Requirements

Several computing and other technological requirements have been highlighted. This includes VoIP, Printer, and Camera Systems. For these requirements, the organization would require a cloud solution to support these requirements. However, this would still involve buying VoIP devices and headphones to support SaaS applications. Such cloud services could include namely Amazon Connect, Microsoft Business Voice, and Google Voice. There are also some options for VoIP services which are also dependent on Telecommunications Service Providers within the region.

For large businesses, Printer and Camera systems would be installed on-premise. Printers will be connected via TCP/IP and appropriate drivers will be installed to user workstations dependent on the type of printer is being installed. Camera systems will be connected to a video recording device on-premise, with an option to transfer the files through file transfer protocols and storage solutions available within the cloud.

Another requirement highlighted was End-Point Security. For large businesses, this will typically involve an Anti-Malware server(s), such as Symantec End-Point Protection Server, in which applicable licenses will be available to be assigned for all users within the organization. The actual end-point security application will then be installed within end-user workstations, and all updates will be centralized and pushed from this server(s).

Intermediary devices must be set up to establish the LAN network within each location within the organization. Devices required include Cisco routers, switches, access points, and relevant security appliances. The security appliances will provide on-premise security against malware, address translation functionalities, and would provide VPN access for remote users outside the organization. Appropriate network subnetting, address allocation, and VLAN assignments must be done while considering designs to implement separate network domains to support the Development, UAT (User Acceptance Testing),

[16] Please do note that as this document's purpose is to serve as a template for designing a Hybrid Cloud Architecture. Thus, some portions of this documentation could be similar to the previous examples on this paper.

and Production environments. This is critical since this is a large organization with hundreds to thousands of end-devices and compute/storage instances. Proper address planning, allocation, and assignment must be considered and should be scalable for future growth. Polices will be implemented using various frameworks as a reference such as GDPR, APEC, NIST, ITIL, COBIT, and ISO to provide system compliance, organizational security, data privacy, and mitigate any risks involving natural or man-made disasters.

A secure and reliable dedicated Internet connection must be obtained from Internet Service Providers (ISP – in a dual-homed configuration) for each branch within the organization to connect to the corporate WAN network, and ultimately, access cloud services to set up the organization's Hybrid Cloud Architecture. The organization must request and reserve several IP ranges such that it can be utilized to support and host public applications and resources to serve its internal users and client base and to deliver ISP and IP connection redundancy within the organization.

Another critical resource is an SMTP server. This enables users to send marketing, advertisement, or application-generated emails which are primary drivers for performing e-mail notifications and campaigns for the organization. There are cloud solutions implementations that would provide SMTP features such as Amazon SES, Azure Plug-in Twilio SendGrid, and GCP Firebase Cloud Messaging.

Critical On-Premise Requirements

In order to support on-premise applications and services, data center design, computing system installation, and delivery must be done.

Application Servers will host all critical applications required for business operations. This could include the local Production, UAT, and Dev resources, which runs applications responsible for executing locally developed applications, web/mobile applications, and stack managers (i.e., MANO – Management and Orchestration tools) that manage and monitor other vital VM instances for the organization. The most critical resources for these devices are Core Processors and Memory. Manipulating these factors will affect the performs of the server and all the VMs hosted within the server. Such servers that can be implemented will include Dell Servers having VMWare Hypervisor configured to enable VM hosting.

Storage Servers will be implemented as a Storage Area Network and provide features that will enable computing instances within servers and workstations within the organization to allocate these virtual hard disk space locally. Redundancy features within the disk arrays, such as with RAID, while performing duplication and high data availability processes such as Striping, Mirroring, or Parity. These redundancy features will then affect the total effective hard disk space that can be utilized, which is the most critical resource for this device.

Such servers that can be implemented will include NetApp FAS, which also offers cloud storage solutions and integration with the AWS, Azure, and GCP.

Database Servers will be delivered to host database instances, which are used in parallel with applications hosted within the Application Server. Maintaining Database availability is critical since this is one of the primary drivers for organizations to perform day to day business operations and to provide services to its client base efficiently. Such server which can be implemented will include Oracle Database.

A modular approach for implementing these environments on-premise should be considered. This is done such that all of the on-premise computing environments within the entire corporate network can be easily orchestrated, managed, and manipulated based on the organization's needs. This approach must be made per site while considering the overall infrastructure of all the branch locations of the organization.

Compute Replication should be performed to the redundant site(s) ahead of time so that any redundant site can easily assume the responsibility to perform the necessary compute operations for the organization. This is done by creating a copy of a compute instance from one of the servers hosting a specific VM instance and cloning it to another remote host device. For the organization to fully implement this Hybrid Cloud Environment that aims to provide Site Redundancy, data synchronization technologies should also be considered to keep up-to-date data and applications between these two sites. This is critical so that if one site fails, all processes can be easily transferred to the alternate site. Once the issues within the site that failed have been resolved, business processes will return to its normal operations (i.e., in line with an organization's Business Continuity and Disaster Recovery Procedures). Several data synchronization tools can be used for on-premise resources that are compatible with AWS, Azure, and GCP, such as Active Data Guard (for Oracle Database Servers) and SnapMirror and Cloud Sync (for NetApp Storage Servers).

Given these computing requirements on-premise, services contained within the private cloud include legacy and highly classified data and application which will not be migrated on the cloud due to technological, sensitivity, and security issues. However, this will also contain all data and applications, which are redundant and synchronized copies of the actual production data and application that would all be hosted on the cloud.

For this organization, it will have two (2) Data Center LAN templates that it would implement to its office locations. The first is with Headquarter Offices, which will host Application, Database, Storage, End-User, Distribution, and Security Networks while the second will be the Branch Offices which would only host Storage, End-User, Distribution and Security Networks. This is done to standardize and efficiently orchestrate services within the enterprise network. All cloud services will then connect to the Data Center LAN through the Internet.

Hosting of Content Delivery through a Community Network

The organization will host its Community Network to external stakeholders to provide access to all relevant information that they would need to continue business processes between them and the organization. This Community Network will be based on Content Delivery, which will provide helpful information about the product and its processing status, product quality assurance initiatives, and other media-based processes that will be delivered through this network. The Community Network can be accessed by each branch location but is primarily managed by the Main Headquarter offices through the cloud.

Critical Cloud Requirements

After capturing the overall information regarding the organization, consideration must be made for the most critical cloud requirements that will require Cloud Services namely Productivity and other essential SaaS tools, IaaS and PaaS deployment and computing instances which would host various services needed to support the organization's business processes which includes application hosting, content delivery, computing system availability and security.

CRM Tools (SaaS) are designed for organizations to better understand the needs and manage the interaction of the organization's client base and its potential customers. AWS, Azure, and GCP provide services for this as a plug-in from other third-party SaaS organizations. An Azure CRM service, namely Dynamics 365, is also a popular choice for systems with integrations with Microsoft. Stand-alone CRM applications, such as HubSpot, Salesforce, Zoho CRM, and LiveChat are also available which has integration to most of these Cloud Service Providers.

E-mail service (SaaS) is a critical tool within organizations to send-out and receive messages to/from external organizations. This is often integrated with Calendaring and Collaboration services within an application running these services. AWS, Azure, and GCP have created solutions for these services, namely the AWS WorkMail, Microsoft Exchange, and Google Mail[17].

Document Processing Tools (SaaS) are applications that allow users to create human-readable files. The most popular tools in today's market are Microsoft Office and Google Drive Services[18].

[17] It should be noted that Microsoft Exchange and Google Mail is the most mature E-mail Services available in the today's market. Organizations will be able to leverage all the integrations available for this service to other compatible services.

[18] Together with all other productivity tools such as E-mails, Calendars and Document Processing makes up Office 365 or Microsoft Suite (i.e., Microsoft) and G Suite (i.e., Google).

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Productivity Service	Amazon WorkMail	Microsoft Exchange and Office	G Suite
Plan	-	Office 365 Business Premium	Business
Data Residency	US and EU	Most Critical Applications located in Hong Kong, Malaysia, and Singapore, with some minor services stored in the US	US and EU
Features	Provides Email services and some Microsoft Service Integration	Includes most critical Productivity applications and some Management Features	Includes most critical Productivity applications, Security and Management Features
Dedicated Mobile Applications	None. Uses Web applications.	Yes	None. Uses Web Applications.

Table 62 – Large Business: Productivity Services

Dedicated services that would enable user access and management are critical for larger organizations. Identity and Access Management (I&AM) (SaaS) is the ability of the system to provide access classification to users within the organization. However, there are also services provided by CSPs such as I&AM that relate not just to users but also with devices. This is done by DHCP servers, which provides appropriate device addressing information for the organization. These features comprise a Domain Controller that performs security authentication and information requests from the organization's domain. Services such as Windows Server, a product suite from Microsoft that includes features such as Active Directory, DHCP, File, and DNS services integrate on-premise resources to the Azure environment. Other CSP providers, such as AWS and GCP, enables integration of their platform to these features as Microsoft is already a robust and proven system that supports Windows workstations, which are the majority of end-user devices utilized within any organization. The following CSP and I&AM services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Large Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Authentication and Access Management Service	I&AM	Active Directory	Cloud IAM
Data Residency	US	Singapore	Singapore/Indonesia
Availability	99.90%	99.90%	99.95%

Table 63 – Large Business: Authentication and Access Management Services

Computing resources (IaaS/PaaS) in the cloud will require a compute instance to host and run applications that will support the business' operations. Such computing instances can host VMs which will then execute processes based on services configured into it. This could include web applications (i.e., public) and stand-alone applications used within the organization (i.e., private). There are other dedicated compute instances the support dedicated purposes such as web hosting, app hosting, containers, serverless architectures, development, big data analytics, batch processing, and other specialized compute requirements (e.g., IoT, AI/ML, Big Data Analytics and Fog Computing). Compute instances are either offered as IaaS or PaaS and depending on which service is utilized based on the needs of an organization, one can select from the other. For this paper, the following IaaS Compute services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Large Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Compute Service	EC2	Virtual Machines	Compute Engine
Data Residency	Singapore/Indonesia	Singapore	Singapore/Indonesia
Availability	99.99%	99.95%	99.99%

Table 64 – Large Business: Compute Services

Cloud storage systems (IaaS) are critical for the organization's business continuity and disaster recovery strategies. It enables the organization to continue business operations in case of natural or man-made disasters affecting the corporate environment. For Large Businesses, Block, File, and Object storage solutions are applicable. File Storage presents information as multiple levels of files organized in folders. Block Storage divides information into arbitrary, organized equal chunks of data. Lastly, Object Storage stores data and associates it with its corresponding metadata. (Red Hat, 2020). For this organization, it will be utilizing all storage systems. File Storage will provide standard file services native to the users through their end-user workstations, Block Storage will be utilized to store and access data efficiently, and Object Storage will be implemented to provide the storage solution for its Content Delivery Service delivered through its hosted Community network. It should be

noted that proper deduplication strategies must be implemented for these solutions to save on storage utilization and costs.

Archival systems (IaaS) are also part of the organization's storage systems. This solution enables organizations to store files that will be left unaccessed for long periods due to the organization's data archival guidelines in compliance with industry standards. AWS and Azure have established Disaster Recovery (DR) services (DRaaS) to solve the BC and DR requirements of an organization. The following Storage and DR Services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Large Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Block Storage Services	EBS	Block Blob Storage	Persistent Disk
Data Residency	Singapore/Indonesia	Singapore	Singapore/Indonesia
Availability	99.90%	99.90%	99.95%

Table 65 – Large Business: Block Storage Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
File Storage Service	EFS	File Storage	Filestore
Data Residency	Singapore/Indonesia	Singapore	Singapore/Indonesia
Availability	99.90%	99.99%	99.90%

Table 66 – Large Business: File Storage Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Object Storage Services	S3	Blob Storage	Cloud Storage
Data Residency	Singapore/Indonesia	Singapore	Singapore/Indonesia
Availability	99.90%	99.90%	99.95%

Table 67 – Large Business: Object Storage Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Archival Services	Glacier	Backup (Blob)	Cloud Storage
Data Residency	Singapore/Indonesia	Singapore	Singapore/Indonesia
Availability	99.99%	99.90%	99.95%

Table 68 – Large Business: Archival Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Disaster Recovery	CloudEndure	Site Recovery	-
Data Residency	Singapore/Indonesia	Singapore	-
RPO/RTO	Seconds to a few minutes	99.90%	-

Table 69 – Large Business: Disaster Recovery Services

Database resources (PaaS) in the cloud will run on a pre-set database operating system that will host critical instances that stores information and receives/replies to queries associated with any operations performed in the application. There are two (2) major structures for databases. These are Relational Databases (SQL) and Non-relational Databases (NoSQL). SQL is a structured database that relies on indexes and the relations of tables and the relation of multiple tables(entities/objects), columns (data sets), and rows (records). As the approach for SQL is more rigid, NoSQL offers greater flexibility and adaptability with the applications that best work with unstructured data models (Williams, 2019). For this organization, it will implement both SQL and NoSQL database solutions based on the needs of a particular application associated with a specific database instance so that application performance will be efficient and optimized.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Relational/SQL Database Services	AWS RDS - Oracle	SQL Database	Cloud SQL
Data Residency	Singapore/Indonesia	Singapore	Singapore/Indonesia
Availability	99.95%	99.99%	99.95%

Table 70 – Large Business: Relational Database Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Non-Relational/NoSQL Database Services	Dynamo DB	Cosmos DB	Cloud Bigtable
Data Residency	Singapore/Indonesia	Singapore	Singapore/Indonesia
Availability	99.99%	99.99%	99.99%

Table 71 – Large Business: Non-Relational Database Services

Similar to the on-premise implementation, a modular approach for implementing these cloud environments should be considered. This is done such that all cloud computing environments can be easily orchestrated, managed, and manipulated based on the organization's needs. This approach must be made per cloud service provider per region per zone (if applicable) while considering the overall infrastructure of all the branch locations of the organization. Compute Replication should be performed between service providers ahead of time so that any redundant service that provides the hosting of the organization's computing system can easily assume the responsibility to perform the necessary computing operations for the organization. This is done by creating a copy of a compute instance from one of the servers hosting a specific VM instance and cloning it to another remote host device from one CSP to another. In order for the organization to fully implement this Hybrid Cloud Environment that aims to provide Site Redundancy, data synchronization technologies should also be considered in order to keep an updated data and application between two CSPs continuously. This is critical so that if one CSP environment fails, all processes can be easily transferred to the other CSP environment. Once the issues within the primary production environment that failed have been resolved, business processes will return to its normal operations (i.e., in line with an organization's Business Continuity and Disaster Recovery Procedures). Several data synchronization tools can be used for cloud resources which are compatible with AWS, Azure, and GCP, such as AWS Simple Workflow, Azure Logic Apps, and GCP Dataflow.

In order to have real-time information regarding all the cloud resources utilized by the organization, Cloud Monitoring and Management services should also be considered. This is useful for monitoring the cloud computing systems' health, determining diagnostic information, and troubleshooting should there be any issues within these resources. The following Cloud Monitoring and Management services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Large Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Cloud Monitoring Services	CloudWatch; CloudTrail	Monitor; Log Analytics	Stackdriver
Data Residency	Singapore/Indonesia	Singapore	Singapore/Indonesia
Availability	99.9%, 99.9%	99.90%	99.95%

Table 72 – Large Business: Cloud Monitoring Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Cloud Management Services	Systems Manager;	Policy; Cost Management	Stackdriver
Data Residency	Singapore/Indonesia	Singapore	Singapore/Indonesia
Availability	99.90%	No SLA	99.95%

Table 73 – Large Business: Cloud Management Services

Networking resources (IaaS/PaaS/SaaS) are essential services that will provide networking functionalities similar to how intermediary devices (such as routers, switches, and other networking appliances) perform processes for the organization. These allow flexibility by utilizing such networking services without the users getting to be familiar with a specific device model such as Cisco, Juniper, and Alcatel. Aside from connecting local and remote resources through routing and switching, these also provide other networking functionalities such as DHCP, DNS, Address Translation, and VPN services. In relation to networking services, compute instances such as Windows Server can also provide services that include DHCP and DNS services. DNS services can also be provided by the organization's ISP upon request and can be accessed from third-party DNS service providers such as Cloudflare. Another critical requirement for this organization is the hosting of a community network that will provide all vital information with regards to the processes and business information for the entire organization, its branches, and all of its stakeholders (i.e., business partners). This CDN will provide an endpoint such that information related to sales, inventory, and product status will be published. For this paper, the following Networking services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Large Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Virtual Private Cloud Services	VPC	Virtual Network; VPN Gateway	Virtual Private Cloud; Cloud NAT
Data Residency	Singapore/Indonesia	Singapore	Singapore/Indonesia
Availability	99.90%	99.95%, 99.95%	99.95%, 99.9%

Table 74 – Large Business: Virtual Private Cloud Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
DNS Services	Route 53	Azure DNS	Cloud DNS
Data Residency	Singapore/Indonesia/Philippines	Singapore	Singapore/Indonesia
Availability	100.00%	100.00%	100.00%

Table 75 – Large Business: DNS Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Lease Line Services	Direct Connect	ExpressRoute	Cloud Interconnect
Data Residency	Singapore/Indonesia	Singapore	Korea
Availability	99.90%	99.95%	99.99%

Table 76 – Large Business: Lease Line Services

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Content Delivery Services	CloudFront	CDN	Cloud CDN
Data Residency	Singapore/Indonesia/Philippines	Singapore	Singapore/Indonesia
Availability	99.90%	99.90%	99.95%

Table 77 – Large Business: Content Delivery Services

Security resources (SaaS) in the cloud provides the organization with high-performance security and flexibility to select which security features and critical resources will be protected. Security resources in the cloud help with Advanced Threat Protection, Risk Mitigation, and Vulnerability Identification. Ultimately, the fundamental purpose of these services is to inspect data coming in and out of the system and classify them according to risk to protect the data of the organization and continue normal business operations. For this paper, the following Security services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Large Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Security Services	GuardDuty; Macie; Shield; WAF	Security Center	Cloud DLP; Cloud Security Scanner
Data Residency	[All] Singapore/Indonesia, [Macie] US	Singapore	Singapore/Indonesia
Availability	[GuardDuty and Macie] 99.9%, [Shield] 100%, [WAF] 99.95%	99.90%	No SLA

Table 78 – Large Business: Security Services

Migration

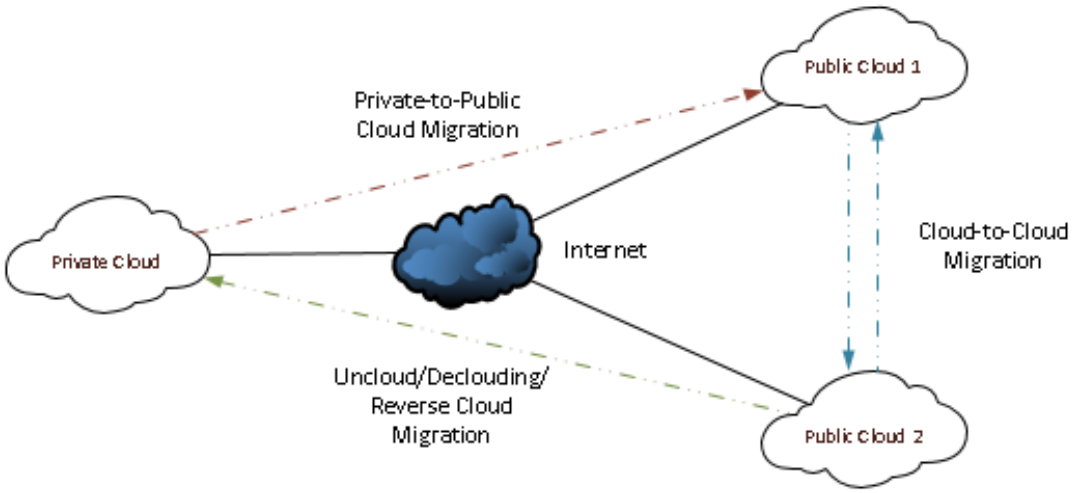

Figure 40 - Cloud Migration

Migration provides the ability for organizations to transfer their computing system from one native environment to another. This could be performed by transferring data and applications through the Internet or through physically transporting devices containing critical resources (i.e., which are typically sized at Terabytes of data for large organizations) to its destination. As highlighted, there are three (3) common types of cloud migrations. These are the Private-to-Public, Public-to-

Public, and Public-to-Private Migration. Private-to-Public Cloud Migration is the shift from utilizing an on-premise cloud environment to a third-party cloud service provider. When an organization has been using a third-party cloud service provider and want to transition to another cloud provider, Public-to-Public or Cloud-to-Cloud Migration must then be considered. Finally, Public-to-Private, Uncloud, Declouding, or Reverse Cloud Migration is the shift from utilizing a third-party cloud service provider to an on-premise cloud solution. (Rouse M. , 2018). Migration is done in order to efficiently gain all the benefits of establishing a Hybrid Cloud Architecture. However, consideration of any migration activities must be planned properly in order to minimize its impact to business operations during and once the system has been completely migrated. In this scenario, the organization will be utilizing Private-to-Cloud Migration and Cloud-to-Cloud Migration to transfer its resources into the cloud. For this paper, the following Migration services have been selected and compared to identify key defining factors that will be used to select the most appropriate service for this Large Business Hybrid Cloud Environment.

Cloud Service Provider	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Migration Services	AWS Database Migration; AWS Migration Hub; AWS Server Migration Service; AWS Snowball; AWS Snowball Edge; AWS Snowmobile	Azure Migrate; Azure Database Migration Services; Data Box	Transfer Appliance; Transfer Service
Data Residency	[All] Singapore/Indonesia, [AWS Migration Hub] US	Singapore	Singapore/Indonesia
Availability	[AWS Database Migration] 99.9%, [All] N/A	N/A	N/A

Table 79 – Large Business: Migration Services

Other Services

As this organization will be utilizing several advanced technologies to ensure that its products, services, and business parameters are all in good standing, adequate technologies must be utilized to deliver these objectives. Technologies such as IoT to monitor merchandise production, Fog Computing for edge data processing, AI/ML for business intelligence, and Data Lakes/Big Data Analytics for monitoring business trends and health are essential to even optimize and deliver efficient business processes to all of the organization's stakeholders.

Analysis

Based on this large business model, the primary goal is to provide secure connectivity and high data availability amongst all office locations across the entire organization. The requirement is needed since all offices are located in various remote locations. The management of the organization is also looking into delivering most legacy applications through the cloud such that it would minimize the total cost of ownership (TCO) of these devices. This was based on the TCO tool utilized by the organization to prove that hosting most of the organization's computing resources will cost less relative to its current setup. Thus, a cost analysis will be disregarded for this model.

The private cloud infrastructure for the main HQ offices and the branch offices will have similar architecture or "template" such that setup, management, and orchestration can be implemented "as a module." This cloud will host some legacy computing resources that are not compatible once migrated over the cloud and are strictly confidential information locally stored and utilized with the enterprise network.

On the other hand, the organization's public cloud(s) will utilize two (2) CSPs that are continuously syncing from one another in an active-passive state such that each CSP will host identical services. This will offer high availability of services in cases of CSP unavailability. The configuration will provide a seamless transition from one CSP to another and will provide minimal to no business impact. This public cloud will also host a content delivery service that will be hosted by the organization by established through a community network within the region. This enables external stakeholders (i.e., business partners such as farmers and retailers) to access and add relevant information regarding business operations.

It should be noted that the individual office locations (i.e., HQ or branch) will have separate LANs for each computing resource type running within that specific office location. A different subnetwork for each department/division occupying individual office locations will also be created. This modular approach will help IT administrators to easily control and adequately analyze the corporate network.

The organization will utilize various Cloud Services, including multiple IaaS, PaaS and SaaS offerings associated with Compute, Storage, Database, and Networking services as well as productivity tools, I&AM, data synchronization compatible with on-premise devices, disaster recovery, migration, security, and cloud service monitoring and management. It will also utilize advanced CSP services related to IoT for business output monitoring, Fog Computing for edge data processing, AI/ML for business intelligence, and Data Lakes/Big Data Analytics for monitoring various business parameters, which are all needed to streamline business operations and analytics between the organization[19].

[19] Please do note that these advanced features will not be discussed further in this documentation.

Location, for which the service stores its information and where it can deliver the actual services should also be considered for these services. Based on the provided information[20], most services considered from these CSPs are hosted in the Asia Pacific region (Singapore and Indonesia) except for the following services:

- Productivity Tools: AWS and GCP host some data in the US
- I&AM: AWS host its services in the US
- Leased Line Services: GCP only offers leased line services in Korea
- Security Services: AWS Macie is hosted only in the US
- Migration Services: AWS Migration Hub is hosted only in the US

Based on the features of each service that will be utilized for this cloud implementation, SLA highlights that services considered from these CSPs will have more than 99% availability in all locations, satisfying the high data and service availability requirements of the organization.

Considering these factors will drive the organization to select the appropriate technologies, setup, and services to implement its requirements and deliver its business operations.

It should be noted that there would be seven (7) main requirements for this organization. This will involve complying with the regional APEC Privacy Framework, establishing high data security, availability and connectivity between office locations, migrating most legacy services in the cloud to reduce cost, hosting a content delivery service through a community network, adopting the most appropriate productivity tools, establishing proper resource permissions and utilizing multiple CSPs to provide business continuity and disaster recovery options for the organization. The compliance with the APEC Privacy Framework will be the management piece that will drive the organization to select which computing solutions could be used to provide necessary data security and privacy features. Data availability and site connectivity will be driven by which technology and services will ultimately be used to deliver all business processes within the organization. To achieve these requirements, the organization will host its services within multiple CSP regions and utilize multiple availability zones. This setup will ultimately provide seamless service recovery and data security and availability, which is of primary importance for this organization.

To establish this, the organization will utilize all CSPs discussed in this documentation with the following characteristics:

- The organization will utilize all AWS and Azure services highlighted in this section except for the archival services
- The organization will utilize all GCP storage services highlighted in this section

[20] For the location information of these services, please see the CSP Services section of this Large Business Modeling and Scenario.

Since data availability and security are crucial to the organization, all critical data utilized by the organization will be replicated and synced to each of these CSP providers, including the on-premise enterprise network. The primary cloud computing capabilities will be hosted through AWS, as the primary site, and Azure, as the secondary site. On the other hand, GCP will become the organization's cloud repository and the main archival solution. This choice is selected since there are no particular Disaster Recovery services offered by GCP. By using this scheme, administrators will have a clear picture of how to efficiently orchestrate the system per CSP per region per availability zones. This will enable the organization to sustain and continue business operations if one Availability Zone, Region, or CSP fails and protect the organization's access to its critical data as it is securely stored within these on-premise and cloud environments.

Based on all the information discussed, this Hybrid Cloud Infrastructure scheme was selected such that it will allow separation and classification of services hosted on these CSPs. Application availability and data security will be delivered through this hybrid cloud approach as AWS will be the primary site, Azure as the redundant site, and GCP as the archival/repository environment for the organization. The choice for this scheme is motivated due to the business continuity and disaster recovery requirements of the organization, its initiatives to migrate most legacy application and host them to multiple CSPs to reduce company costs and maintenance, and to provide high data security and availability. To manage enterprise user access, permissions, and roles, and provide collaborative and productivity tools, the organization will be utilizing Azure's I&AM and productivity services, effectively making the organization adapt to the Microsoft Suite. For these cloud services, it is offered using a pay-as-you-go model, such that no complex licensing processes will be made, which aids with managing all the services and related subscriptions to such services. However, this is different for some on-premise services such that proper licensing rules and auditing must be initiated to comply with that device vendors' licensing standards and related terms of agreements.

It should be noted that not the best services must be used in a hybrid cloud architecture implementation as there are also several factors outside of the scope of this study that affects the selection of cloud services in any organization. Appropriate frameworks, such as the combined AWS and Microsoft architecture framework can be used to streamline further and enhance the efficiency of the operations going forward.

Section 5: Conclusion and Recommendations

It was highlighted in this documentation that increasing management, maintenance, technological upgrade, operational and capital costs brought by excessive energy needs, limitation in system provisioning driven by server sprawl, variable resource utilization, rising system complexity and need for specialized personnel to support these computing resources, drive for process simplification, intelligence and automation, and market competition are but some of the primary challenges being faced by any IT organization. Cloud Services provides a solution for these issues as it provides a platform for more efficient use of computing resources, on-demand provisioning/de-previsioning, scalability, flexibility, agility, and saves on cost through a pay-as-you-go model. (Bojanova & Samba, 2011)

Service sharing through Cloud Computing is the current phase in which computing technologies are driven to enhance service performance and streamline operations for enterprise organizations globally. In order to reap the full potential of these technologies/services, proper factors must be considered to design a Hybrid Cloud Architecture for any organization's infrastructure. Some of these factors include the business needs, costs, legal guidelines, data residency requirements, and disaster recovery services to keep up with the organization's operations, workflows, business continuity, and disaster recovery objectives and procedures.

Advantages in utilizing Cloud Services include less investment in expensive hardware and software, increased computing resource utilization efficiency, and borderless/on-demand access without the need to worry about system management. Aside from private organizations, governments and the public sector do realize the "flexibility, operational benefits, and substantial cost savings that cloud computing can provide." There are, however, some doubts about its cost efficiency, computing robustness, and service availability. Some business organizations, such as McKinsey's & Co. (i.e., one of the world's trusted management consulting firms) reported that cloud services are best used only for small to mid-size enterprises (SMEs) and questioned model sustainability with larger enterprise organizations. AWS, which got hit by a lightning strike, was unable to deliver its AWS EC2 service to its clients that caused numerous application downtimes. With regards to security, a bad actor was able to get into the GCP's Google Apps which enabled them to acquire confidential information. Lastly, Greenpeace reported that there could be energy and sustainability implications brought by these data centers which consume large amounts of energy. (Bojanova & Samba, 2011)

These controls are compensated by following several model frameworks such as the AWS Well-Architected Framework, Microsoft Solutions Framework, Microsoft Operations Framework, and Zachman Framework in order to deal with and further improve the security, operational efficiency, reliability, agility and cost optimization of such services that will be utilized to design an enterprise Hybrid Cloud Architecture.

The pace of technological advancement increases every year and businesses need to keep up with these changes to develop a competitive advantage among other industry players. By utilizing Cloud Services and establishing a Hybrid Cloud Architecture, proper planning of architecture design, deployment schemes, and process analysis must be made to optimize the delivery of solutions based on the business needs of any organization, regardless of size or maturity.

From this documentation, a framework in design that considers the metrics below is used to appropriately design a Hybrid Cloud Architecture through utilizing CSPs, namely AWS, Azure, and GCP. The most critical parameter below is determining the business requirements. All other parameters are but constraints which will drive the selection of technology and services used to deliver solutions accordingly. This is a critical step towards creating any Hybrid Cloud Architecture.

- Business Requirements
- Capital and Costs
- Legal Compliance
- Setup and Management
- Engineering Time
- Licensing
- Data Availability (HA)
- Disaster Recovery (DR)
- Security

Once a clear picture about what the business needs are, proper consideration of the deployment model must be considered. In order to proceed with a Hybrid Cloud Architecture, a primary site that will deliver the core of day-to-day business operations must be established. This could include the basic computing resources (in terms of user end-devices and applications), storage requirements (through NAS or SAN), database resources (to support application and API processing), networking services (to connect all devices within the primary enterprise LAN – i.e., Private Cloud) and security services (to mitigate risks within the organization's computing environment). The next step for this is to branch out of this primary LAN environment and utilize the services offered through the Public Cloud. In this documentation, we have utilized AWS, Azure, and GCP as the CSPs that could be used to carry out these requirements. This cloud adoption can be done through several phases per computing resources/services or can be developed all at the same time (e.g., site/service duplication and migration) delivered through IaaS, PaaS, and SaaS service models. This varies per business requirement, constraints, priorities, and timelines in which the organization requires the solutions to be readily available and functional.

Based on the cases highlighted on this documentation for small, medium and large organizations, we can see that the main factors that drove the selection to cloud service to deliver business solutions are primarily the business requirements and constraints, cost optimization and efficacy, and the consolidating of services under a centralized management system. Business requirements are the initial inputs in designing any Hybrid Cloud Environment as this is the primary driver that initiates the selection on what type of services should be utilized, where the data should be located, and how these integrated computing systems solve the organization's requirements. The highlighted metrics above are some of the requirements that Hybrid Cloud Experts could consider during this design delivery. Cost is the driving factor to select which services will be utilized to deliver the business needs and if they will be utilizing public cloud services at all or not based on the TCO comparison of hosting all these computing systems relative to the on-premise or collocation implementation. Finally, the last factor is System Consolidation and Management. In order to simplify management and orchestration, IT administrators should consider using a centralized and unified solution so that no additional issues with regards to technology integration and compatibility will be experienced once the services have been finally selected and undergone implementation. This will reduce associated costs by removing wasted man-hours on troubleshooting several services offered from different

cloud platforms. By realizing the business requirements, cost, consolidation, and management, business solutions provided will be enhanced, robust, agile, and efficient.

As the analysis piece and based on the design and deployment methods that will be used to realize business solutions, a framework should be utilized in order to further enhance any solutions provided to an organization. For this documentation, a framework that combines the Amazon Well-Architected, Microsoft Solutions, and Microsoft Operations Framework is utilized in order to create a more optimized, agile, and robust infrastructure that will support and deliver the Hybrid Cloud Architecture.

However, we should also do note that this documentation is limited in context as this would not be able to discuss all information in full detail. This includes some specialized services that were not utilized and the simplification of cost analysis. Moreover, supplementary resources are provided to add valuable information for topics that are out of scope for this study.

“Cloud computing is no longer on the horizon; it has become the next logical step in enterprise computing. Organizations are focusing on managing information and no longer on managing infrastructure, by having their applications and storage, applications development environments, and even infrastructure and security available from the Cloud.” (Bojanova & Samba, 2011)

By developing this Hybrid Cloud Architecture Design, Deployment and Analysis documentation, it could be used as a basic template in designing an actual hybrid cloud environment for any organization.

[This page is left intentionally blank]

Section 6: References

Academind. (2018, July 25). *SQL vs NoSQL or MySQL vs MongoDB*. Retrieved from https://www.youtube.com/watch?v=ZS_kXvOeQ5Y

Akamai. (2019). Retrieved from Public Cloud or Private Cloud?: https://www.akamai.com/uk/en/resources/public-private-cloud.jsp

Aucoin, J. (2019, April 8). *CBTnuggets*. Retrieved from AWS vs Azure vs Google: Cloud Wars 2019: https://www.cbtnuggets.com/blog/certifications/microsoft/aws-vs-azure-vs-google-cloud-wars-2019

AWS - Architecture. (2019). *Amazong Well-Architected.* Retrieved from https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

AWS - Cloud Service. (2020). *AWS Documentation*. Retrieved from AWS: https://docs.aws.amazon.com/index.html?nc2=h_ql_doc_do

AWS - Global Infrastructure. (2019). *Global Infrastructure*. Retrieved from AWS: https://aws.amazon.com/about-aws/global-infrastructure/?p=ngi&loc=0

AWS - Service Level Agreements. (2019). *Service Level Agreements*. Retrieved from AWS: https://aws.amazon.com/legal/service-level-agreements/

AWS - Shared Responsibility Model. (2019). *Shared Responsibility Model*. Retrieved from AWS: https://aws.amazon.com/compliance/shared-responsibility-model/

Azure - Cloud Services. (2020). *Azure Products*. Retrieved from Microsoft Azure: https://azure.microsoft.com/en-ca/services/

Azure - Global Infrastructure. (2020). *Azure Global Infrastructure*. Retrieved from Microsoft Azure: https://azure.microsoft.com/en-gb/global-infrastructure/

Azure - Security. (2019, October 15). *Shared Responsibility in the Cloud*. Retrieved from Microsoft Azure: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Barcos, R. (2019, July 27). Cloud & Platform Support Engineer. (K. Soliven, Interviewer)

Bojanova, I., & Samba, A. (2011). Analysis of Cloud Computing Delivery Architecture Models. *Workshops of International Conference on Advanced Information Networking and Applications011 Workshops*, (p. 6). Kent and Adelphi, USA.

Cisco NetAcad, C. (2019). Connecting Networks - Chapter 7.2. North America.

Cloud Standard Customer Council. (2016, February). Practical Guide to Hybrod Cloud Computing.

Dell. (2020). *Company Overview*. Retrieved from Dell: https://corporate.delltechnologies.com/en-us/about-us.htm

Duffy, S. (2019). Udemy: A-Z 300 Azure Arcchitecrure Technologies Certification Exam.

EDUCBA. (2019). *Cloud Computing vs Fog Computing*. Retrieved from EDUCBA.

ERPINNEWS. (2018, January 19). *Fog computing vs edge computing*. Retrieved from ERPINNEWS: https://erpinnews.com/fog-computing-vs-edge-computing

GCP - Cloud Locations. (2020). *Cloud Locations*. Retrieved from Google Cloud: https://cloud.google.com/about/locations/

GCP - Cloud Services. (2020, February 3). *Google Cloud Platform Services Summary*. Retrieved from Google Cloud: https://cloud.google.com/terms/services

GCP - Google Security Overview. (2020). *Google Security Model*. Retrieved from Google Cloud: https://cloud.google.com/security/overview/

GCP - Service Level Agreements. (2020). *Google Cloud Platform Service Level Agreements*. Retrieved from Google Cloud: https://cloud.google.com/terms/sla/

Giraldeau, A. (2019, October 28). Data Center Architecture. (K. Soliven, Interviewer) Edmonton, Alberta, Canada.

Grance, T., & Mell, P. (2011). *National Institute of Standards and Technology.*

Hanyes, T. (2018, May 22). Prepare for the Death of the Data Center as We Know It. Gartner.

HCL. (2019). Retrieved from TECHNOLOGY Q&A: https://www.hcltech.com/technology-qa/what-is-cloud-architecture

Intellipaat. (2019, January 24). *AWS vs Azure vs GCP | Amazon Web Services vs Microsoft Azure vs Google Cloud Platform | Intellipaat*. Retrieved from Youtube: https://www.youtube.com/watch?v=n24OBVGHufQ

Jain, G. (2019, February 9). *Traditional Data Center v/s Cloud Data Center*. Retrieved from eMoneyIndeed: https://www.emoneyindeed.com/traditional-data-center-vs-cloud-data-center/

Kavis, M. (2018, April 6). *Clearing the air around cloud shared responsibility models*. Retrieved from Deloitte: https://www2.deloitte.com/us/en/pages/consulting/articles/clearing-the-air-around-cloud-shared-responsibility-models.html

Kroonenburg, R. (2019). Udemy: AWS Certified Solutions Architect - Associate 2019.

Kulikova, O., & Sturrus, E. (2014, June). Orchestrating Hybrid Cloud Deployment: An Overview. IEEE Computer Society. doi:0018-9162/14

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). *National Institure of Standards and Technology.*

Maloy, J. (2012, August 9). *Tableau Community Forums: What is the difference between core-based and user-based licenses?* Retrieved from Tableau: https://community.tableau.com/thread/119461

Microsoft - MOF. (2008, April 8). *Microsoft Docs*. Retrieved from Microsoft Operations Framework 4.0: https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc506049(v=technet.10)?redirectedfrom=MSDN

Microsoft - MSF. (2004, April 9). *Microsoft*. Retrieved from Microsoft Solutions Framework Version 3 White Papers: https://www.microsoft.com/en-ca/download/details.aspx?id=13870

Microsoft Azure. (2019). Retrieved from What are public, private, and hybrid clouds?: https://azure.microsoft.com/en-ca/overview/what-are-private-public-hybrid-clouds/

MuleSoft. (2020). *What is an API? (Application Programming Interface)*. Retrieved from MuleSoft: MuleSoft

NetApp. (2020). *FAS Storage Systems*. Retrieved from NetApp FAS Storage System Resources: https://www.netapp.com/us/documentation/fas-storage-systems.aspx

Odun-Ayo, I., Ananya, M., Agono, F., & Goddy-Worlu, R. (2018, August 20). Cloud Computing Architecture: A Critical Analysis. *2018 18th International Conference on Computational Science and Applications (ICCSA)* (p. 7). Melbourne, VIC, Australia: IEEE. doi:10.1109/ICCSA.2018.8439638

Owen. (2019, April 11). *Otava*. Retrieved from Public vs. Private Cloud Computing: https://www.otava.com/reference/public-vs-private-cloud-computing/

Patrizio, A. (2019, January 22). *Datamation*. Retrieved from AWS vs. Azure vs. Google: Cloud Comparison [2019 Update]: https://www.datamation.com/cloud-computing/aws-vs-azure-vs-google-cloud-comparison.html

Raza, M. (2018, September 12). *bmc blogs*. Retrieved from Public Cloud vs Private Cloud vs Hybrid Cloud: What's The Difference?: https://www.bmc.com/blogs/public-private-hybrid-cloud/

Red Hat. (2020). *Storage*. Retrieved from Storage: File storage, block storage, or object storage?: https://www.redhat.com/en/topics/data-storage/file-block-object-storage

Rouse, M. (2018, September). *TechTarget*. Retrieved from cloud migration: https://searchcloudcomputing.techtarget.com/definition/cloud-migration

Rouse, M., Stedman, C., Lavery, T., Sirkin, J., & Kruggel, C. (2017, August). *Relational database management system guide: RDBMS still on top*. Retrieved from SearchOracle: https://searchoracle.techtarget.com/definition/Oracle

Sakovich, N. (2018, September 10). *Fog Computing vs. Cloud Computing for IoT Projects*. Retrieved from Sam Solutions: https://www.sam-solutions.com/blog/fog-computing-vs-cloud-computing-for-iot-projects/

Strickland, J. (2008, April 8). *Howstuffworks*. Retrieved from How Cloud Computing Works: https://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm

Techopedia. (2020). *What is NetApp Storage*. Retrieved from NetApp Storage: https://www.techopedia.com/definition/30461/netapp-storage

Tonner, A. (2018, May). Forrester Opportunity Snapshot: Pivotal And Microsoft - Hybrid Cloud Demands Consistency.

Tsang, A. (2019, August 6). Chief Information Officer. (K. Soliven, Interviewer)

VMware. (2020). Retrieved from VMware: https://www.vmware.com/

Watts, S., & Raza, M. (2019, June 15). SaaS vs PaaS vs IaaS: What's The Difference and How To Choose. Retrieved from https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

White, J. (2014, May 5). *Expedient*. Retrieved from Private vs. Public Cloud: What's the Difference?: https://www.expedient.com/blog/private-vs-public-cloud-whats-difference/

Whitehouse, L. (2008, September 8). *The pros and cons of file-level vs. block-level data deduplication technology*. Retrieved from SearchDataBackup: https://searchdatabackup.techtarget.com/tip/The-pros-and-cons-of-file-level-vs-block-level-data-deduplication-technology

Wikipedia. (2019, August 14). Retrieved from Amazon Web Services: https://en.wikipedia.org/wiki/Amazon_Web_Services

Wikipedia. (2019, July 5). Retrieved from Cloud computing architecture: https://en.wikipedia.org/wiki/Cloud_computing_architecture

Wikipedia. (2019, July 17). Retrieved from Google Cloud Platform: https://en.wikipedia.org/wiki/Google_Cloud_Platform

Wikipedia. (2019, August 7). Retrieved from Microsoft Azure: https://en.wikipedia.org/wiki/Microsoft_Azure

Wikipedia. (2019, November 5). *As a service*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/As_a_service

Williams, T. (2019, July 11). *Relational SQL vs. Non-Relational NoSQL Databases*. Retrieved from Dev: https://dev.to/trevoirwilliams/relational-sql-vs-non-relational-nosql-databases-hi5

Zachman, J. (2008). *Zachman International Enterprise Architecture.* Retrieved from The Concise Definition of The Zachman Framework by: John A. Zachman: https://www.zachman.com/about-the-zachman-framework?ref=wellarchitected-wp

Section 7: Appendix

Public Cloud Services

The following are the Public Cloud services that are utilized for this documentation. All services came from CSPs, namely AWS, Azure, and GCP. The following descriptions are taken from their respective organization's documentation. For more details with regards to these services, please refer to the following resources:

For AWS:

- AWS Documentation
- AWS Cloud Products

For Azure:

- Azure Products

For GCP:

- Google Cloud Platform Services Summary

Computing Services

Virtual Machine

Azure offers an on-demand and scalable computing resource called Azure Virtual Machines (VM). Without buying or maintaining physical hardware that runs it, Azure VM gives users the versatility of virtualization. However, one still needs to configure, patch, and install the software that runs on it in order to maintain the VM. (Azure - Cloud Services, 2020)

Compute Engine

Compute Engine allows users to create and run virtual machines on Google infrastructure. It provides scaling, performance, and value, which allows launching large compute clusters on Google's infrastructure with ease. No advance investments are needed, and one can expect to run thousands of virtual CPUs on a fast and strongly consistent-performing system. (GCP - Cloud Services, 2020)

EC2

Amazon Elastic Compute Cloud (Amazon EC2) is a cloud service that gives a secure and resizable compute capacity in the cloud. It intends to make web-scale cloud computing simpler for developers. Amazon EC2's straightforward web service interface enables one to gain and configure capacity with minimal friction. (AWS - Cloud Service, 2020)

Block Storage

Block Blob

Block blob storage is utilized for streaming and keeping data such as documents, videos, pictures, backups, and other unstructured text or binary data. (Azure - Cloud Services, 2020)

Persistent Disk

Google Persistent Disk is a superior block storage for Google Cloud Platform. It provides SSD and HDD storage, which can be connected to instances running in either Compute Engines or Google Kubernetes Engines. Storage volumes offer the capacity to help simultaneous readers and can be transparently resized and backed up fast. (GCP - Cloud Services, 2020)

EBS

Amazon Elastic Block Store (EBS) is a simple, superior block storage service intended for use with Amazon Elastic Compute Cloud (EC2) for throughput and transaction-intensive workloads at any scale. A broad scope of workloads is used widely on Amazon EBS, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytic engines, file systems, and media workflows. (AWS - Cloud Service, 2020)

File Storage

File Storage

Azure Files provides completely managed file shares in the cloud accessed in the industry-standard Server Message Block (SMB) protocol. Its file shares can be mounted simultaneously by cloud or on-premises deployments of Windows, Linux, and macOS. Also, its shares can be cached on Windows Serves with Azure File Sync for quick access close to where the data is being used. (Azure - Cloud Services, 2020)

Cloud Filestore

Cloud Filestore is a managed file storage service for applications that require a filesystem interface and a shared filesystem for data. Filestore gives users a simple, native experience for standing up managed Network Attached Storage (NAS) with their Google Compute Engine and Kubernetes Engine instances. The ability to fine-tune Filestore's performance and capacity independently leads to predictably fast performance for the user's file-based workloads. (GCP - Cloud Services, 2020)

EFS

Amazon Elastic File System (Amazon EFS) gives a straightforward, versatile, and entirely managed elastic NFS file system that can be used with AWS Cloud services and on-premises resources. It is designed to scale on-demand to petabytes without interrupting applications, automatically grows and shrinks as one add and remove files, and eliminates the need to arrange and manage capacity to accommodate growth. (AWS - Cloud Service, 2020)

Object Storage

Blob Storage

Microsoft's object storage answer for the cloud is the Azure Blob storage. It is developed to store massive quantities of unstructured data. Unstructured data does not attach itself to a particular data model or definition, such as text or binary data. (Azure - Cloud Services, 2020)

Cloud Storage

Cloud Storage offers global, secured storage that scales to exabytes of data. One can easily access data from any storage class, integrate storage into one's applications with a single unified API, and effectively improve price and performance. (GCP - Cloud Services, 2020)

S3

Amazon Simple Storage Service (Amazon S3) is a storage service that gives industry-leading scalability, data availability, security, and performance. This implies that clients of all sizes and industries can use it to store and ensure any amount of data for a variety of uses, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics are secured. Amazon S3 gives simple management features so one can organize data and arrange access controls to meet one's specific business, organizational, and compliance requirements. It is intended for 99.999999999% (11 9's) of durability and keeps data for millions of applications for companies around the world. (AWS - Cloud Service, 2020)

Archival Storage

Backup

Azure Backup service gives a straightforward, secure, and cost-efficient solutions to back up and recover data from the Microsoft Azure cloud. (Azure - Cloud Services, 2020)

Cloud Storage

Cloud Storage offers global, secured object storage that scales to exabytes of data. One can access information easily from any storage class and integrate this storage into one's applications with a single unified API, and effectively optimize cost and performance. (GCP - Cloud Services, 2020)

Glacier

Amazon S3 Glacier and S3 Glacier Deep Archive are the protected, durable, and extremely low-cost Amazon S3 cloud storage class for data storage and long-term backup. They are optimized to deliver 99.999999999% durability and offers extensive security and compliance abilities that can aid to meet the most stringent regulatory requirements. Customers can keep data for $1 per terabyte per month, a considerable saving in comparison with on-premises solutions. Amazon S3 Glacier gives three options to access archives from a few minutes to several hours, while S3 Glacier Deep Archive provides two access options from 12 to 48 hours to minimize cost. (AWS - Cloud Service, 2020)

Disaster Recovery Services

Site Recovery

Azure Site Recovery is used for disaster recovery of on-premises workloads, and Azure VMs. (Azure - Cloud Services, 2020)

Cloud Endure

CloudEndure Disaster Recovery is an AWS service that allows shifting disaster recovery strategy to the AWS cloud from occurring physical or virtual data centers, private clouds, or other public clouds fast and straightforward. One can additionally ensure protection to mission-critical workloads, if one has already migrated to AWS, with cross-region disaster recovery. (AWS - Cloud Service, 2020)

Virtual Private Cloud

Virtual Network

Azure Virtual Network (VNet) is a significant structure for one's private network in Azure. VNet allows many types of Azure resources, like Azure Virtual Machines (VM), to safely communicate with one another, the internet, and on-premises networks. VNet is the same as a traditional network where one would operate in one's own data center, but it brings additional advantages of Azure's infrastructure like scale, accessibility, and isolation. (Azure - Cloud Services, 2020)

VPN Gateway

A VPN gateway is a particular type of virtual network gateway used to deliver encrypted data transfer between an Azure virtual network and an on-premises site over the public Internet. One can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network. Every virtual network can only have one VPN gateway. However, one can make multiple connections to the same VPN gateway. When one creates multiple VPN gateway connections, all VPN tunnels share the available gateway bandwidth. (Azure - Cloud Services, 2020)

Virtual Private Cloud

Google Cloud Virtual Private Cloud (VPC) gives networking functionality to Compute Engine virtual machine (VM) occurrences, Google Kubernetes Engine (GKE) containers, and the App Engine flexible conditions. VPC offers networking for one's cloud-based resources that are global, scalable, and flexible. (GCP - Cloud Services, 2020)

Cloud NAT

Cloud NAT, a Network Address Translation service managed by Google cloud, permits one to arrange applications without public IP addresses while also allowing access to the internet for updates, patching, config management, and more with control and efficiency. External resources cannot directly access any private instances behind the Cloud NAT gateway, which helps to keep Google Cloud VPCs isolated and secured. (GCP - Cloud Services, 2020)

VPC

Amazon Virtual Private Cloud (Amazon VPC) allows one to arrange a logically separated section of the AWS Cloud, where one can open AWS resources in a virtual network that users can define. Users have complete control over their virtual networking environment, which includes their IP address range, subnets creation, and configuration of route tables and network gateways. One can use both IPv4 and IPv6 in one's VPC for secured and accessible resources and applications. (AWS - Cloud Service, 2020)

Leased Line Services

ExpressRoute

ExpressRoute allows one to expand on-premises networks into the Microsoft cloud over a direct private connection (e.g., any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location facility) facilitated by a connectivity provider. With ExpressRoute, one can build more reliability, faster speed, consistent latencies, and secured connections versus typical connections over the Internet connections to Microsoft cloud services. (Azure - Cloud Services, 2020)

Cloud Interconnect

Cloud Interconnect increases one's on-premises network to Google's network through a highly available, low latency connection. One can use Dedicated Interconnect to connect to Google or use Partner Interconnect to connect to Google through a supported service provider. (GCP - Cloud Services, 2020)

Direct Connect

AWS Direct Connect is a cloud service solution that establishes a dedicated network connection from one's premises to AWS. Using AWS Direct Connect, one can create a private connection between AWS and one's datacenter, office, or colocation environment, which can reduce network cost, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connection. (AWS - Cloud Service, 2020)

Content Delivery Network

CDN

Azure Content Delivery Network (CDN) is a global CDN solution for conveying high-bandwidth content. It may be hosted in Azure or any other location. One can cache static objects loaded from Azure Blob storage, a web application, or any public web server, using the closest point of presence (POP) server using Azure CDN. It can also accelerate dynamic content, which cannot be cached by leveraging different network and routing optimizations. (Azure - Cloud Services, 2020)

Cloud CDN

Cloud CDN (Content Delivery Network) makes use of Google's globally distributed edge points of presence to cache HTTP(S) load balanced content close to one's users. To provide fast delivery of content to users while reducing serving costs, caching content at the edges of Google's network is completed. (GCP - Cloud Services, 2020)

CloudFront

Amazon CloudFront is a fast content delivery network (CDN) service that securely transports data, videos, applications, and APIs to customers worldwide with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is incorporated with AWS, both physical locations that are connected directly to the AWS global infrastructure. CloudFront also works with services such as AWS Shield for DDoS mitigation, Amazon S3, Elastic Load Balancing, or Amazon EC3 as origins for applications and Lambda Edge to run custom code closer to customers' users and to alter the user experience. Lastly, using AWS services such as Amazon S3, Amazon EC2, or Elastic Load Balancing would not cost the users as they transfer data between these services and CloudFront. (AWS - Cloud Service, 2020)

DNS Services

Azure DNS

Azure DNS is a hosting service for DNS domains providing domain name resolution. One can manage one's DNS records by using the same credentials, APIs, tools, and billing by hosting one's domains in Azure. (Azure - Cloud Services, 2020)

Cloud DNS

Google Cloud DNS is a scalable, dependable, and managed authoritative Domain Name System (DNS) service running on the same infrastructure as Google. It has low latency, high availability, and is a cheaper way to make one's application and services available to users. One can quickly publish and manage millions of DNS zones and records using the simple user interface, command-line interface, or API. (GCP - Cloud Services, 2020)

Route 53

Amazon Route 53 is a highly accessible and scalable cloud Domain Name System (DNS) web service. It is established to give developers and businesses a reliable and cheaper way to route end users to Internet applications by translating names. (AWS - Cloud Service, 2020)

Relational Database

Azure SQL Database

Provided as a managed service, Azure SQL Database is a general-purpose relational database. With it, one can create a high-performance data storing layer for the applications and solutions in Azure. SQL Database can be the right choice for different modern cloud applications as it enables one to process-relational and non-relational structures like graphs, JSON, spatial, and XML. (Azure - Cloud Services, 2020)

Cloud SQL

Cloud SQL is compatible with applications that use MySQL, PostgreSQL, and SQL Server. One can connect with nearly any application, anywhere in the world. It automates backups, replication, and failover to ensure one's database is reliable, accessible, and flexible to one's performance needs. (GCP - Cloud Services, 2020)

RDS

Amazon Relational Database Service (Amazon RDS) allows easy setup, operations, and scalability to a relational database in the cloud. While automating time-consuming administration tasks like hardware provisioning, database setup, patching, and backups, it provides cost-efficient and resizable capacity. To give a fast performance, high accessibility, and compatibility needed, Amazon RDS frees a user to focus on applications. (AWS - Cloud Service, 2020)

Non-relational Database

Cosmos DB

Microsoft's globally distributed, multi-model database service is Azure Cosmos DB. It enables one to elastically and independently scale throughput and storage across any number of Azure regions worldwide. One can elastically scale throughput and storage, and take advantage of fast,single-digit-millisecond data access using one's favorite API with SQL, MongoDB, Cassandra, Tables, or Gremlin. For throughput, latency, accessibility, and consistency guarantees, something no other database service offers Cosmos DB provides comprehensive service level agreements (SLAs). (Azure - Cloud Services, 2020)

Cloud Bigtable

Google's NoSQL Big Data database service is Cloud Bigtable. It is a database service that executes many core Google services, including Search, Analytics, Maps, and Gmail. Cloud Bigtable is a less populated table that scales billions of rows and thousands of columns, which enables them to store terabytes or even petabytes of data. Cloud Bigtable is best for storing large amounts of single-keyed data with very low latency. It supports high read and write throughputs at low latency, an ideal data source for MapReduce operations. (GCP - Cloud Services, 2020)

Cloud Datastore

Cloud Firestore is a NoSQL document database created for automatic scaling and high-performance application development. Firestore is the newest version of Datastore, which introduces several improvements over Datastore. In the future, every existing Datastore database will be upgraded automatically to Cloud Firestore in Datastore mode. (GCP - Cloud Services, 2020)

DynamoDB

Amazon Dynamo DB is a key-value document database delivering single-digit millisecond performance at any scale. It is a fully managed, multi-region, multi-master, durable database with built-in security, backup and restore features, and in-memory caching for internet-scale applications. (AWS - Cloud Service, 2020)

Monitoring

Monitor

Azure Monitor takes advantage of the availability and performance of one's applications and services by bringing a comprehensive answer for collecting, analyzing, and acting on telemetry from one's cloud and on-premises environments. (Azure - Cloud Services, 2020)

Log Analytics

Log Analytics is a web service used to write and execute Azure Monitor log queries. It starts with a new blank query and is opened by selecting Logs in the Azure Monitor Menu. (Azure - Cloud Services, 2020)

Stackdriver

Stackdriver is Google Cloud's embedded observability suite created to monitor, troubleshoot, and improve cloud infrastructure, software, and application performance. It enables users to efficiently build and run workloads, keeping applications performant and available. (GCP - Cloud Services, 2020)

CloudWatch

Amazon CloudWatch monitors and observes service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. It provides users with data and actionable insights to monitor applications, respond to system-wide performance changes, improve resource utilization, and get a unified view of operational health. It also collects monitoring and operational data in the form of logs, metrics, and events that gives a unified view of AWS resources, applications, and services that run on AWS and on-premise servers. (AWS - Cloud Service, 2020)

CloudTrail

AWS CloudTrail enables governance, compliance, operational auditing, and risk auditing of one's AWS account. One can log, continuously monitor and retain account activity related to actions across an AWS infrastructure with CloudTrail. It gives event history of one's AWS account activity, including actions seen through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. The even history enables simplification of security analysis, resource change tracking, and troubleshooting. One can also use CloudTrail to check unusual activity in one's AWS accounts. All these services help to simplify operational analysis and troubleshooting. (AWS - Cloud Service, 2020)

Management

Policy

Azure Policy is used to create, assign, and manage policies. To stay compliant with corporate standards and service level agreements, different rules and effects over one's resources are applied. (Azure - Cloud Services, 2020)

Cost Management

Take advantage of the tools found in one's Azure subscription to get more value out of the cloud and implement financial governance in one's organization. (Azure - Cloud Services, 2020)

System Manager

AWS Systems Manager provides visibility and regulation of one's infrastructure on AWS. Systems Manager offers a unified user interface so one can view operational data from multiple AWS services and allows one to automate operational tasks across one's AWS resources. One can group resources such as Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances with Systems Manager by applying and viewing operational data for monitoring and troubleshooting, and taking action on one's groups of resources. Systems Manager shortens the time to spot and resolve operational problems, simplifies the management of resource and application, making it easy to operate and manage one's infrastructure securely at scale. (GCP - Cloud Services, 2020)

Management Console

The Console enables cloud management for all aspects of one's AWS account, which includes monitoring monthly expenditure by service, handling security credentials, or even setting up new IAM Users. (AWS - Cloud Service, 2020)

Security

Security Center

Azure Security Center supports the security posture of one's data centers, providing advanced threat protection across one's hybrid workloads in the cloud, whether they are in Azure or not, and also on-premises as it is a unified infrastructure security management system. (Azure - Cloud Services, 2020)

Cloud DLP

Cloud DLP gives access to a sensitive data inspection, classification, and de-identification platform. (GCP - Cloud Services, 2020)

Cloud Security Scanner

Web Security Scanner recognizes security weaknesses in one's App Engine, Compute Engine, and Google Kubernetes Engine web applications. It crawls one's application, which follows all links within the scope of one's starting URLs and attempts to apply as many user inputs and event handlers as possible. (GCP - Cloud Services, 2020)

GuardDuty

Amazon GuardDuty is a service that detects threats and continuously monitors for malicious activity and illegal behavior in order to protect one's AWS accounts and workloads. (AWS - Cloud Service, 2020)

Macie

Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in AWS to provide security services. It distinguishes sensitive data such as personally identifiable information (PII) or intellectual property and provides dashboards and alerts that provide visibility into how data is accessed or moved. (AWS - Cloud Service, 2020)

Shield

AWS Shield is a Distributed Denial of Service (DDoS) protection services that protects applications running on AWS. It offers an always-on detection and automatic inline mitigations that decrease application downtime and latency. The two tiers of AWS Shield are Standard and Advanced. (AWS - Cloud Service, 2020)

WAF

AWS WAF is a firewall that protects web applications or APIs against common web exploits that may affect accessibility, compromise security, or consume extra resources. It gives control over how traffic reaches one's applications by enabling the creation of security guidelines that block common attack patterns, such as SQL injections or cross-site scripting, a and rules that change specific traffic patters one define. (AWS - Cloud Service, 2020)

Access Management

Active Directory

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access organization service that helps employees sign in and access resources relating to the entries below. (Azure - Cloud Services, 2020)

- External resources, like Microsoft Office 365, Azure Portal and thousands of other SaaS applications
- Internal resources, like apps on one's corporate network and intranet, including any cloud apps developed by one's organization.

Cloud IAM

Cloud IAM allows granular access to specific Google Cloud resources and prevents access to other resources. It allows the adoption of the security principle of least privilege, where one can only grant necessary permissions to access specific resources. (GCP - Cloud Services, 2020)

IAM

AWS Identity and Access Management (IAM) allows management access to AWS services and resources securely. One can create and manage AWS users and groups and use permissions to allows and deny access to AWS resources. (AWS - Cloud Service, 2020)

Directory Service

AWS Directory Service for Microsoft Active Directory or AWS Managed Microsoft AD, it allows directory-aware workloads and AWS resources to apply managed Active Directory in the AWS Cloud. AWS Managed Microsoft AD is created on the actual Microsoft Active Directory and does not need synchronization and replication of one's data from an existing Active Directory to the cloud. (AWS - Cloud Service, 2020)

Migration

Azure Migrate
Azure Migrate provides a centralized hub to assess and migrate on-premises infrastructure, application, and data to Azure. (Azure - Cloud Services, 2020)

Azure Site Recovery
Use Azure Site Recovery for disaster recovery of on-premises workloads, and Azure VMs. (Azure - Cloud Services, 2020)

Azure Database Migration Services
Azure Database Migration Service is a managed service that enables seamless migrations from multiple database sources to Azure Data platforms providing minimal downtime. (Azure - Cloud Services, 2020)

Data Box
The Azure Data Box family offers products of different storage capacities to help send terabytes (TB) of data to Azure in a quick, inexpensive, and reliable way. Microsoft accelerates secure data transfer by shipping the client its proprietary storage devices that enable offline or over the network data transfer. (Azure - Cloud Services, 2020)

Transfer Appliance
Transfer Appliance is set up in one's data center which is a secured, rackable high capacity storage server. One can fill it with data and sends it to an ingest location where data is uploaded to Google Cloud Storage. (GCP - Cloud Services, 2020)

Transfer Service
A broad-scale of online data transfers from online and on-premises sources to Cloud Storage. (GCP - Cloud Services, 2020)

AWS Database Migration
AWS Database Migration Service allows the migration of databases to AWS quickly and securely. During the migration, the source database continues to fully operate to decrease downtime to applications that rely on the database. (AWS - Cloud Service, 2020)

AWS Migration Hub

AWS Migration Hub gives a single location to track the status of application migrations through multiple AWS and partner solutions. It permits one to choose the AWS and partner migration tools that suitable to one's needs while giving accessibility to the status of migrations across one's portfolio of applications. (AWS - Cloud Service, 2020)

AWS Server Migration Service:

AWS Server Migration Service (SMS) is an agentless service making it easier and faster for users to transfer thousands of on-premises workloads to AWS. It permits one to automate, schedule, and track incremental replications of live server volumes, which makes it easy for users to manage large-scale server migrations. (AWS - Cloud Service, 2020)

AWS Snowball

Snowball is a petabyte-scale data transport solution which devices created to protect the transfer of vast quantities of data into and out of the AWS Cloud. It addresses common problems with large-scale data transfers such as high network costs, long transfer times, and security concerns. (AWS - Cloud Service, 2020)

AWS Snowball Edge

AWS Snowball Edge comes in two options, which are highlighted below. (AWS - Cloud Service, 2020)

- Snowball Edge Storage Optimized - provides both block storage and Amazon S3 compatible object storage and 24 vCPUs. It is appropriate for local storages and large scale data transfer.
- Snowball Edge Compute Optimized - provides 52 vCPUs, block, and object storage and an optional GPU for innovative machine learning and full-motion video analysis in disconnected environments.

AWS Snowmobile

AWS Snowmobile is an Exabyte-scale data transfer service utilized to move increased amounts of data to AWS. One can move up to 100PB per Snowmobile. It allows a less complicated movement of massive volumes of data such as video libraries, image repositories, and complete data center migration to the cloud. (AWS - Cloud Service, 2020)

Summary of Keys to Success

The following are key factors that can be used to fulfilling business requirements and delivering business solutions to the organization. The following descriptions are taken from the Cloud Standard Customer Council – Practical Guide to Hybrid Cloud Computing documentation, which is a collaborative effort from various organizations such as IBM, Ernst a& Young (EY), and other management and consulting organization to bring together insights about cloud service adoption. (Cloud Standard Customer Council, 2016)

Key Factor	Description
1. Identify the design and cloud deployment model to deliver business needs	● Determine the right resource model – on-premises private cloud, hosted private cloud, or public cloud ● Rationalize application and data environment ● Apply decision criteria to define the right deployment model – flexibility, security, speed & automation, cost, locality, service levels, and system interdependencies ● IT architects consider options for application placement in the hybrid cloud (see four options)
2. Integrate cloud services with existing computing systems	● Put in place controlled interfaces by which components in cloud services can access applications and data in on-premises systems – consider technologies such as API Management ● Consider the administration and business aspects of the integration as well as the functional integration of the systems ● Demand that the cloud service provider supports standards for the interfaces to their cloud services
3. Address any peering and other related connectivity policies	● Consider the requirements of each link between components that spans two or more cloud services or on-premises system and ensure that appropriate connectivity is available to support those requirements ● Consider the use of network virtualization if available ● Ensure that the connectivity capabilities can support resilience and disaster recovery requirements
4. Develop governance and management policies along with service agreements	● Assess existing compliance and governance frameworks, identify gaps and harmonize processes

	● The need for thorough and efficient change management and communications increases with the addition of multiple cloud service providers ● Allow adequate time to educate and habituate changes across the organization ● Identify gaps in measurement and management visibility
5. Risk assessment relative to security and related privacy issues	● Understand the interfaces between components running in private cloud services, in public cloud services and on-premises and apply appropriate and consistent security controls to each of them ● Evaluate the location of all datasets in the hybrid cloud deployment and ensure the application of consistent access controls and encryption ● When migrating application components between environments, be careful to check that the security controls in place for the new environment meet or exceed those in place for the old environment ● Apply technologies across all the environments that are part of the hybrid cloud deployment such as I&AM systems
6. Hybrid Cloud environment management	● Enable management of the complete hybrid cloud system, spanning all the environments used ● Either adapt and integrate existing on-premises management tools or consider the use of new cloud-based management services, based on cost and functionality ● Look for APIs and integration points for management capabilities rather than fixed-function management applications

Table 80 - Summary of Keys to Success in a Hybrid Cloud Architecture
(Cloud Standard Customer Council, 2016)