Modern Operating Systems - Operating System Upgrade Proposal

Table of Contents

[Project Outline 4](#_Toc482128964)

[Company Profile 4](#_Toc482128965)

[Summary of current Operating systems for Server and Client 4](#_Toc482128966)

[Proposal 5](#_Toc482128967)

[OS Processor and Core (Week 1) 5](#_Toc482128968)

[Benefits 5](#_Toc482128969)

[Steps 6](#_Toc482128970)

[Requirements 6](#_Toc482128971)

[Scheduling Algorithms (Week 2) 7](#_Toc482128972)

[Transition from Nonvirtual Environment to Virtual Environment 7](#_Toc482128973)

[Scheduling Algorithm 8](#_Toc482128974)

[Benefits and Challenges 9](#_Toc482128975)

[OS Concurrency Mechanism (Week 3) 10](#_Toc482128976)

[Distributed Computing Environment for Samyang 10](#_Toc482128977)

[Message Passing through RPC 11](#_Toc482128978)

[Communication and Synchronization through Message Passing 12](#_Toc482128979)

[OS Security Risk and Mitigation Strategy (Week 4) 13](#_Toc482128980)

[Risk Assessment in Virtual Environments 13](#_Toc482128981)

[Qualitative Threat Assessment: 14](#_Toc482128982)

[Identifying Vulnerabilities in Virtualized Operating System 15](#_Toc482128983)

[Hypervisor. 15](#_Toc482128984)

[Virtual Machines. 15](#_Toc482128985)

[File Sharing Between Host and Guests. 16](#_Toc482128986)

[Snapshots. 16](#_Toc482128987)

[Network Storage. 16](#_Toc482128988)

[Risk Mitigation Approach 17](#_Toc482128989)

[Hypervisor. 17](#_Toc482128990)

[Virtual Machines. 18](#_Toc482128991)

[File Sharing Between Host and Guests. 18](#_Toc482128992)

[Snapshots. 18](#_Toc482128993)

[Network Storage. 19](#_Toc482128994)

[Future Considerations Using Emerging Technology (Week 5) 19](#_Toc482128995)

[Emerging Technology/Architecture 20](#_Toc482128996)

[Enterprise Strategic Requirements 21](#_Toc482128997)

[Potential Benefits 22](#_Toc482128998)

[References 24](#_Toc482128999)

# Project Outline

## Company Profile

Samyang, a sugar manufacturer in Korea, has more than 50 years of history with over 500 employees worldwide. Samyang is running the ERP (Enterprise Resources Planning) solution, Oracle’s JD Edwards EnterpriseOne Xe release for more than ten years (JDEE1Tips, 2015). This aged client-server model has incurred high maintenance cost for both server and client machines. So this proposal is to explore the possible upgrade opportunity of both Enterprise Solution and its operating system.

According to Smartbridge, there are four main considerations which justify application upgrade, which are support considerations, functional considerations, technical considerations and performance considerations (Smartbridge, 2017). Based on the change made in the application area, which naturally requires more powerful and stable platform to run this resource hungry application package.

Naturally, the upgrade of hardware and the upgrade of the operating system require a new approach to get the best crop in the market, which is, virtualization and cloud. So to maximize the capacity and minimize the cost of maintenance, we suggest Samyang would implement the Windows 2016 Server on multiprocessor and multicore machines.

## Summary of current Operating systems for Server and Client

Currently, the server platform for enterprise solution is Windows Server 2008 R2 upgraded in 2010 from Windows Server 2003. Though 2008 R2 has better security feature, increase productivity, and reduce administrative overhead, it still leaves room for another upgrade for Samyang to move to virtualization than Windows Server 2003 (Microsoft, 2009).

For end-users, the company has upgraded operating to Windows 7 from Windows XP in 2010, excluding JDE developers, because Windows XP is an only operating system for development work.

## Proposal

It is high time for Samyang to look into the opportunity of upgrading the operating system to Windows Server 2016. This new operating system has multiple enhancements with features like Security built-in at the start, enablement to move to the cloud with Hyper-V, low storage cost is some of them, let alone enhanced performance (Microsoft, 2016).

Especially Hyper-V on Windows Server 2016 has a typical benefit for virtualization like shared virtual hard disks, shielded virtual machines, start order priority for clustered virtual machines, and so on (Davies, 2017).

Virtualization and Cloud are new to Samyang, which have advantages, a failure of one virtual machine does not disrupt the whole system, less hardware requirement which saves money substantially, easier maintenance for load balancing and multiple servers), even older version can be running through the image of XP (Tanenbaum, 2015). And this configuration or approach can maximize multiprocessor and multicore operating systems as discussed further below.

# OS Processor and Core

## Benefits

The benefit Samyang can gain through upgrade the operating system to Windows 2006 Server along with the latest hardware is crucial to have competitive edge against competitor as below,

* Centralized server for all different enterprise solutions with multiple processors which have multi-cores
* Minimize system downtime through enhanced system performance
* Enablement for flexible working through tablet and smartphone which frees time and space constraints
* Decrease the ownership of hardware by exploring the possible route to cloud service or private cloud service provided by software vendors
* Centralized configuration and monitoring through Hyper-V which is equivalent to hypervisor in much other literature

## Steps

To maximize the possible benefit of the latest operating systems, firstly, check the features and services that each enterprise solutions provide: check memory requirement of it, the number of kernels and processes available for these applications, and review the benefit to subscribing cloud service provided by the application vendor.

Currently, the vendor provides services with Information-as-a-Service, Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Services (Oracle, 2016). However, migration to the cloud can be considered in next phase of an upgrade though it may have significant saving regarding cost.

## Requirements

New operating system and hardware must support multi-threading capability for multiple servers with multiprocessor and multicore processors because multiple kernels in later enterprise solution support multithreading to have better performance by eliminating global variables in calling request. So in a single box,

* Windows Server 2016 R2 to handle batch applications, business functions, and database server in a single operating system
* Web Server 64-bit Edition of Red Hat Enterprise Linux 5 with version Oracle WebLogic 11gR1 to handle presentation layer request from HTML client
* Additional server with the same platform for EnterpriseOne Application Interface Services (AIS) Server for mobile client
* A Same operating system for business service (BSSV) which enables EnterpriseOne application to communicate with third party software through XML
* A BI (Business Intelligence) Enterprise Server for reporting
* And lastly, Windows Server 2012 R2 for the deployment server which is used to build the package and deploy it to every server when there is any change in objects related (Oracle, 2017).

Additionally, the new machine has megabytes of cache to the processor chip, and these CPUs need to have multiple complete CPUs to support concurrent processing requested by 500 concurrent users and other services.

Lastly, the new system requires a big enough main memory because the application instructions grow bigger for the last ten years of time.

# Scheduling Algorithms

## Transition from Nonvirtual Environment to Virtual Environment

The latest enterprise application release 9.2 is highly distributed environments as described above. Even though the definition of client and server is comparative one, it requires servers for logic which is dedicated to interactive applications, a batch server for batch jobs, JAS for HTML client, BSSV to communicate with different software, BIP which deals with Oracle middleware, AIS for mobile client and so on.

To be benefited from modern operating system technology, virtualization is a way to go. Because virtualization allows a single computer to host multiple virtual machines, each potentially running a completely different operating system (Tanebaum, 2015).

The benefit of virtualization for this configuration is enormous regarding stability, cost saving for hardware, scalability, even this configuration allows the user to run legacy system which requires different operating system. In turn, this configuration requires tight scheduling algorithm to have maximum performance which is not negotiable for daily transactions.

## Scheduling Algorithm

To have a successful upgrade of operating systems for multiple servers to improve overall performance and to load distribution/balance in the future virtual environment, we need to review operating system’s process scheduling algorithm.

In this virtual environment for Samyang, two major systems are interactive system and batch system which are to run on two different operating systems through virtualization. So to meet this aim below,

* Interactive System: response time, and proportionality (or user feel the system is faster enough) for interactive system
* Batch System: throughput, turnaround time, and CPU utilization

Utilizing the round-robin schedule algorithm, and the nonpreemptive priority scheduling algorithm can be suitable respectively (Tanenbaum, 2015). Or these two methods can be compatible with the configuration where Samyang is on because the former is the most basic algorithm and the latter is putting priority in it without a preemptive clock.

## Benefits and Challenges

In general, round robin can be useful for the time-sharing system or transaction processing (Stalling, 2014). Because each process is assigned a time interval, or quantum, as long as a certain process is permitted to run (Tanenbaum, 2015). However, this algorithm leaves a question on the length of the quantum supposing that switching process is expensive to deal with saving and loading registers and memory maps, updating various tables and lists, flushing and reloading the memory cache, and so on (Tanenbaum, 2015).

The challenge of this algorithm is how to compromise between process switch and CPU efficiency or utilization. Another shortcoming of this algorithm is when a certain process has to deal with both processor-bound routine and I/O-bound process routine due to the slowness of I/O. The round robin algorithm can be unfair to processor-bound routines because it allocates the same quantum for both (Stallings, 2014).

Since round robin algorithm gives an equal share to all processes, this can be unfair when there are different types of process. So to have different process schedule algorithm, we can discuss the nonpreemptive priority scheduling algorithm. Where the decision mode of the nonpreemtive is that once a process is in the Running state, it continues to execute until it terminates unless the process blocks itself to wait for I/O or to request some OS service (Stallings, 2014). And the priority-based process scheduling, the scheduler only gives control to a particular process if no other process of higher priority is currently in the Ready state. Commonly this algorithm can be used by grouping the same types of processes to give a certain priority.

However, this algorithm can be challenging in setting priority whether it is static or dynamic. By setting a constant value for priority during the creation of the process, one can cause the waste of CPU usage because no process wants to give in. So to overcome this drawback, priorities can also be assigned dynamically to make the operating system to fulfill certain goals. Supposing that there are some processes which are highly I/O-bound and spend most of their time waiting for I/O to complete. Then the process scheduler would give CPU immediately. This way this process can perform its next I/O request.

Another flaw of this algorithm is that the lowest priority process can starve to death when there is a steady supply of higher priority (Stallings, 2014).

So there is no perfect process scheduling algorithm, and various scheduling algorithms are less significant in a multiprocessor system of a virtual machine environment because of more cores or processors in a single operating system (Stallings, 2014).

# OS Concurrency Mechanism

## Distributed Computing Environment for Samyang

Currently, Samyang is running the enterprise solution, JD Edwards Xe release, which is a client-based client/server model. This configuration requires the dedicated network and higher hardware specification on each client machine whereas the most of the time the highly capable server is idling. Now Samyang is on the verge of taking next steps to the virtualization until they arrive at the cloud computing environment the ultimate goal for the most of the enterprise.

The distributed system is similar to multicomputers which have multiple processors and cores with multiple nodes which have their private memory, without having shared physical memory, so we can call the distributed computing environment as loosely coupled multicomputers which each node represents individual computers (Tanenbaum, 2015). Where the nodes of a distributed system can have different operating systems, and each of them can have own file systems. This configuration is essential for Samyang because this upgrade proposal is the upgrade of applications to JD Edwards EnterpriseOne 9.2 release on top of the operating system upgrade.

From enterprise applications point of view, this configuration is the distributed computing system, but in reality, all these servers are to be sitting on a virtual host because the virtualization is the right path to the cloud environment which is the final aim to have a competitive edge in daily business. To have higher availability, load balancing, and open to scalability, this host will be equipped with Failover Clustering in Windows Server 2016 (Microsoft, 2016). Simply put, a cluster works as a group of interconnected computers which behavior like a single machine (Stallings, 2014).

## Message Passing through RPC

A distributed system connecting multiple computers, the operating systems involve heavily in communication than in computation. So it is very crucial to synchronize the multiple processes through proper communication mechanism in an organization. Some open-ended questions are how to pass a message from one machine/process to anther, how two or more processes do not go into each others’ way, and how to set priority when a certain process is dependent on others.

Commonly, the concurrency in distributed computing environment can be performed using distributed message passing through remote procedure call (RPC) (Stallings, 2014). The distributed message passing in distributed computing environment is more of less same with the message passing in interprocessor communication (IPC) in a computer system which enables data exchange and invocation of functionality residing in a different process, or computer ((Microsoft, 2003).

So a remote procedure call is a variation of the basic message passing model, which is the method of encapsulating communication in a distributed system. An RPC allows kernels on different computers to interact using simple procedure call/return semantics, likewise two processes on a single machine. So this communication method is a refinement of reliable, blocking message passing (Stallings, 2014).

## Communication and Synchronization through Message Passing

Now, going back to the topics on interprocess communication (IPC) to discuss communication and synchronization, where mutual exclusion sustains higher synchronization and communication is crucial to use shared resources. Some fundamental questions arise to deal with communication which applies to both a single computer and multicomputer in distributed computing environment. Some mechanisms come under the consideration of race conditions (where multiple threads or processes read and write a shared data item, and the final result depends on the relative timing of their execution) (Stallings, 2014). To avoid the race condition, and deadlock, the concept of mutual exclusion which requires the critical region/section (only one process accesses to the shared resources) comes to the picture, but a certain situation ends in mutual exclusion with busy waiting (or spin lock). Likewise, the TSL (Test and Set Lock) instruction which locks the bus (communication path) not to allow other CPUs to access the shared area result into the spin lock (Tanenbaum, 2015).

In discussing synchronization and (interprocess) communication, message passing is the most common implementation in distributed computer environments as well as in shared-memory multiprocessor systems. The message passing is using two primitives, send and receive, which is like (the system call) semaphores and unlike (the language construct) monitors (Tanenbaum, 2015). Since the semaphore depends on the shared memory, so it is not suitable for a distributed computing systems. And same goes to the monitors which can utilize a mutex or a binary semaphore. So the message passing mechanism suites for the distributed computing environment, which is working based on an agreement between sender and receiver that the receiver sends a special acknowledgment message back to the sender as soon as the message is received.

Therefore, the distributed message passing through remote procedure call (RPC) is a viable approach for Samyang to have a successful transition to enterprise solution upgrade as well as the operating systems upgrade.

# OS Security Risk and Mitigation Strategy

## Risk Assessment in Virtual Environments

The goal of security in the information systems comprises confidentiality, integrity, and availability (CIA). A *Confidentiality* is concerned with having secret data remain secret (where the threat is the exposure of data). An *Integrity* means that unauthorized users should not be able to modify any data without the owner’s permission (where the threat is the tempering of data). And lastly, an *availability* means that nobody can disturb the system to make it unusable (where the threat is the denial of service) (Tanenbaum, 2015).

To assess the risk in the virtualization, briefly reviewing the definition to assess risks in the information systems.

* A *Threat*: The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability
* A *Threat-Source*: Either (1) intent and method targeted at the intentional exploitation of vulnerability or (2) a situation and method that may accidentally trigger a vulnerability (Elky, 2006)
* *Vulnerability*: a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source (NIST, 2012).

### Qualitative Threat Assessment:

|  |  |  |  |
| --- | --- | --- | --- |
| Risk (source/event) | Vulnerabilities | Likelihood | Impact |
| Software > Operating System / Conduct Denial of Service Attack | Hypervisor | High | Very High  Loss of Availability |
| IT Equipment > Processing, Or Software>Operating System / Exploit poorly configured or unauthorized information systems exposed to the Internet | Virtual Machines | High | Very High  Loss of Availability and Integrity |
| Accidental > User, Or Software Operating System / Perform network sniffing of exposed networks | File Sharing Between Host and Guest | High | High  Loss of Confidentiality |
| Software > Operating System / Gather information using open source discovery of organizational information | Snapshot | High | High  Loss of Confidentiality and Integrity |
| IT Equipment > Storage, Or Communications / Compromise organizational information systems to facilitate exfiltration of data/information | Network Storage | High | High  Loss of Confidentiality and Availability |

Note: Above table follows the guide given by NIST (National Institute of Standards and Technology). This assessment excludes the threat source related with Adversarial and Environmental, NIST classifies 3 tier risk with Tier 1 (Organization Level), Tier 2 (Business Process Level), and Tier 3 (Information system level). The values Very High, High, Moderate, Low, and Very Low are for impact scale for qualitative value (NIST, 2012). The likelihood is defined with Low (0-25% chance of successful exercise of threat during a one-year), Moderate (26~75%), and High (76~100%).

## Identifying Vulnerabilities in Virtualized Operating System

This section is to cover the risk or vulnerability discussed in the risk assessment.

### Hypervisor.

The role of the hypervisor can be 1. *Safety*: the hypervisor should have full control of the virtualized resources. 2. *Fidelity*: the behavior of a program on a virtual machine should be identical to that of the same program running on bare hardware. 3. *Efficiency*: much of the code in the virtual machine should run without intervention by the hypervisor (Tanenbaum, 2015).

The hypervisor is the entry point to the virtualization, so it is positioned with the highest risk if exploited. For instance, Hyper-V exposes a *remote code execution* vulnerability when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. An attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code (Rapid, 2017).

### Virtual Machines.

In virtualized environment, the host operating system can support some virtual machines (VM), each of which has the characteristics of a particular OS and, in some versions of virtualization, the characteristics of a particular hardware platform (Stallings, 2014). However, the characteristics of VM can have loophole as such,

* Allowing the attacker to bypass physical security; hard to control user-specific applications
* Numerous protocol is available
* Any clipboard functionality in VM can be medium for malware (Infosec, 2012).

There is some interesting news article on the *virtual machine escape* which is the process of breaking out of a virtual machine and interacting with the host operating system (Goodin, 2017).

### File Sharing Between Host and Guests.

File and file system is one of the important parts of operating systems because it exists for long-term, it can be shared between processes, and it has it’s own structure (Stalling, 2014). So It is common to share files in the distributed environment. However, in the virtual environment, in sharing file between host and guest in the virtual environment, the compromised guest can access host file system which can disrupt confidentiality and integrity of data. Furthermore, the file sharing can be performed through clipboard or drag and drop, which gives a good chance to exploit this sharing mechanism.

### Snapshots.

A snapshot is a “point in time image” of a virtual guest operating system (VM). That snapshot contains an image of the VMs disk, RAM, and devices at the time the snapshot was taken. With the snapshot, you can return the VM to that point in time, whenever you choose (VirtualizationAdminin.com, 2008).

The risk can be coming when reverting snapshots, any configuration made can be lost including the security settings and audit log for access.

### Network Storage.

In virtualized environment, Network Attached Storage (NAS) is a data storage mechanism that uses special devices connected directly to the network media. These devices are assigned an IP address and can then be accessed by clients via a server that acts as a gateway to the data, or in some cases allows the device to be accessed directly by the clients without an intermediary (Bird, 2002).

Commonly, the network media can be Fibre Channel and iSCSI (Internet Small Computer System Interface). Both Fibre Channel and iSCSI are making use of clear text protocols, which in turn, could be vulnerable to attack. For instance, sniffing tools to read or record storage traffic (Infosec, 2012). According to F-Secure, same goes to a QNAP (Quality Network Appliance Provider) which can be vulnerable to a command injection too (Adam, 2017).

## Risk Mitigation Approach

Mitigation involves fixing the flaw or providing some applicable control to reduce the likelihood or impact associated with the flaw (Elky, 2006). Here we briefly review some of the prevention methods based on the vulnerability discussed above. These methods are considered as recommendations or best practices to minimize the risk.

### Hypervisor.

The hypervisor is the entry point for the virtualization. So the security in the hypervisor is more related with how to control the access, especially through the untrusted network (e.g., the Internet). It is important to disallow the users/processes from getting access to the management functions (GUI, API, login, etc.), and even strictly disable user processes from accessing the host by diverting it to the users VMs (Cox, n.d.). Some recommendations from Microsoft are: Keep the host OS secure. Use a secure network. Secure storage migration traffic. Configure hosts to be part of a guarded fabric. Secure device. Secure hard drive. Harden the Hyper-V host operating the system, grant appropriate permissions. Configure anti-virus exclusions and options for Hyper-V, and so on (Microsoft, 2016).

### Virtual Machines.

To minimize the possible attack in VM layer, there are a number of things to keep in mind. Not to have virtual machine escape, VM is not supposed to be placed on storage, backup or management networks that are connected to the hypervisor. VMs should not directly access a VM data store or repository. Any VMs that process protected information are isolated from other VMs. Do not allow VM to access or view the resources used by the kernel or host. Possibly, use a *virtual appliance* likewise Amazon’s EC2 cloud (Tanenbaum, 2015).

Some other approaches can be: Enable discrete device assignment if needed for a specific workload. Deploy virtual machines with shielding enabled and deploy them to a *guarded fabric* (Microsoft, 2016).

### File Sharing Between Host and Guests.

This topic is largely related to the mitigation approaches in Hypervisor and VMs as described above.

Additionally, set file permission between the host and guests. Set up logging and time synchronization. Encrypt all traffic between clients and hosts, between management systems and the hypervisor, and between the hypervisor and hosts using SSL. Secure IP communications between two hosts by using authentication and encryption on each IP packet. Do not use default self-signed certificates as they’re vulnerable to man-in-the-middle attacks (Infosec, 2012).

### Snapshots.

This action is more related to the privilege and access control to perform snapshot activities. To tackle the vulnerability in snapshot which can cause the denial of service or other types of attack, possibly, disallow the guest OS image from having write access. So the capability of the snapshot is limited to the hypervisor.

Some recommendation from Microsoft is that if the virtual machine runs a server workload in a production environment, take the virtual machine offline and then use Hyper-V Manager to apply or delete the snapshots. To delete snapshots, you must shut down the virtual machine to complete the process (Microsoft, 2010).

### Network Storage.

Numerous mitigation strategies exist for this subject because the storage holds the result of all enterprise activities. Some well know approached are, locate it at dedicated storage networks or non-routable VLANs. Use IPSec to encrypt iSCSI traffic to prevent snooping. Use physical switches to detect and disallow IP or MAC address spoofing. Traffic to and from storage repositories needs to be isolated from non-storage traffic. Security for Fibre Channel uses zoning (Infosec, 2012).

Same repeats in hardening the Hyper-V host (Microsoft, 2016). MAC Address Spoofing, Access Control Lists, DHCP Guard, Port Mirroring, Isolation, VM transmit rate limits are some examples.

# Future Considerations Using Emerging Technology (Week 5)

A sugar manufacturer Samyang has maintained the business under the protection given by the government through monopolizing the business so far. However, this external is to be changed in the competition with other global sugar manufacturers who have more advanced technologies and systems, so it is important to understand the emerging computing technologies to survive from competition. Firstly, Samyang needs more Enterprise Solutions CRM, ERP, SCM, and Planning and Forecasting tools which are fully integrated each other (Software integration) to synchronize the flow of information from the front to the end. Secondly, Samyang needs to adopt the emerging computing technologies which to be discussed in following sections. These trends may shed lights on the diversity on the business positively.

Meanwhile, it is meaningful to list up the low-level emerging technologies which Samyang must be aware of. Some are related to the computing environment, but others are loosely related to it. According to the InformationWeek, Homomorphic Encryption, Fog Computing, Biometrics, Next Generation Wireless Communication, and Human-Robot Collaboration in the Workplace (Froehlich. 2015). On the other hand, the IEEE suggests Nonvolatile Memory, Cyber-Physical Systems (CPS), Data Science, Capability-based Security, Advanced Machine Learning, Network Function Virtualization (NFV), and Containers (IEEE, 2016). The other trends in common are, Bots, Glitches, Backdoors, Drone lanes, Quantum computing, and Augmented knowledge (Webb, 2015). And these lists continue, and most of these technologies impact our daily life to some extent.

## Emerging Technology/Architecture

Here we review three high-level emerging computing technologies in detail, the subject matters are the server virtualization, big data, and cloud computing.

*The server virtualization* is a part of this upgrade proposal and the central element to move to big data and the cloud computing (Stallings, 2014). A bare machine with Hyper-V for Samyang can host many different enterprise solutions they need, and some of them are to be running different operating systems, on a single platform. In short, the host operating system can support many virtual machines which can have certain characteristics of a particular the operating systems and, in specific versions of virtualization, even the peculiarity of certain hardware platform features.

*Big Data* is one of the hottest topics likewise data science now. Some other terms Deep Data, or Smart Data can be used for the same (Favliscak, 2014). The enterprise solutions for Samyang carry many different types of data both structured and unstructured ones for the transactions using e-Commerce, CRM, ERP, and SCM, which can be used for the proper planning and forecast when the data are analyzed properly. To many, Deepmind’s AlphaGo shows the big data with good algorithm come as a shock when AlphaGo beats the top Go player in 2016.

The *Cloud Computing* is the design of software applications that makes use of Web-based on-demand service and the provision of management infrastructure that cover functions as computational resources provisioning, workload balancing and performance monitoring (Lin & Shih, 2010). Some characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service (NIST, 2011).

## Enterprise Strategic Requirements

To implement the successful emerging technologies in the future, possibly Samyang needs an agile and flexible upgrade for now.

First of all, *the server virtualization* is an integral part of an upgrade to continue to run multiple enterprise solutions at lower cost, which convert current independent servers to the virtual machines. To expand the database server capabilities, potentially implement the Oracle Database Appliance (ODA) which is an affordable engineered system with clustering and highly scalable which is offered by software vendor Oracle. According to Oracle (Oracle, 2017).

Secondly, open the possibility of implementing *big data* in due course based on the database system by centralizing all different business data collected through the enterprise solutions within Samyang. To support scalable big data stores and processing, the infrastructure should be able to support the easy addition of new resources. This scalable database system is to be operational and analytics databases, which extends to implement database and analytics (NIST, 2015).

Lastly, to lead this upgrade to the *cloud computing*, Samyang implement the virtualization proactively. Some believe that cloud computing is still in its infancy and that it will continue to expand to replace other forms of individual operating systems and computing. Challenges with cloud computing (such as security, privacy, redundancy, and so forth) will need to be addressed in current upgrade. Other past challenges have been resolved, such as scalability, operating system (OS) upgrades, sharing resources, accessibility from anywhere, and more (CTU, 2017).

## Potential Benefits

To survive and thrive in the current competitive sugar market in the globe, the upgrade to the Virtualization, preliminary Big Data, and the Cloud Computing are discussed. Now, the tangible benefit of these emerging technologies are:

The primary benefits of *server virtualization* are:

* Reduce the number of servers (ultimate case, a single machine can hold many virtual machines).
* Reduce the Total Cost of Ownership (TCO, the costs of hardware, maintenance, power, and air conditioning).
* Improve availability and business continuity (e.g., live migration).
* Increase efficiency for development and test environments (multiple operating systems) (NEC, n.d.).

These benefits directly related to the security benefit in virtualization (centralized storage, isolated VMs, hardware reduction, desktop virtualization, server virtualization, hypervisor security and so on) (Infosec, 2012).

On the other hand, the importance of *big data* is not about how much data currently have, rather what can be done with it. The potential benefits of big data are: 1) Cost reductions, 2) Time reductions, 3) New product development and optimized offerings, and 4) Smart decision making. Hence, big data is combined with high-powered analytics, it is possible to accomplish business-related tasks:

* Determine the root causes of failures, issues, and defects in near-real time.
* Generate immediate promotional benefit based on the clients’ spending habit.
* Recalculate entire risk portfolios in minutes.
* Detect fraudulent behavior before it affects organization (SAS, 2017).

Lastly, the benefit of the *cloud computing* can be abstracted using, as many of the marketing documents read:

* Flexibility (extends scalability, various storage options – private, public or hybrid, control choices – XaaS, and security features provided by cloud computing vendors ).
* Efficiency (virtual desktop through an internet connection, get applications quicker, data security by isolating database, savings on equipment which is resulted from virtualization, pay per usage), and the strategic value (streamlined work, regular update by the host, collaboration.
* Competitive edge to the competitors who are not in the cloud computing) (IBM, 2017).

# References

Adam. (2017). New NAS Vulnerabilities are as Bad as they Get. Retrieved April 30, 2017, from <https://safeandsavvy.f-secure.com/2017/04/12/new-nas-vulnerabilities-are-pretty-much-as-bad-as-they-get/>

Bird, D. (2002). Network Storage – The Basics. Retrieved April 30, 2017, from <http://www.enterprisestorageforum.com/technology/features/article.php/947551/Network-Storage---The-Basics.htm>

Colorado Technical University. (2017). Cloud Computing. Retrieved May 8, 2017, from <https://class.ctuonline.edu/_layouts/MUSEViewer/Asset.aspx?MID=7267268&aid=7267278>

Cox, P. (n.d.). Top virtualization security risks and how to prevent them. April 29, 2017, from <http://docs.media.bitpipe.com/io_10x/io_100160/item_409004/CAE-guide2.pdf>

Davies, K. et al. (2017). What's new in Hyper-V in Windows Server 2016. Retrieved April 08, 2017, from <https://technet.microsoft.com/en-us/windows-server-docs/compute/hyper-v/what-s-new-in-hyper-v-on-windows>

Elky, S. (2006). An Introduction to Information System Risk Management. SANS Technology Institute. Bethesda, MD. Retrieved April 28, 2017, from <https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204>

Favliscak, Pamela,M.A., M.S. (2014). Big data, deep data, smart data. Information Outlook (Online), 18(3), 12-14. Retrieved from <http://search.proquest.com.proxy.cecybrary.com/docview/1542129490?accountid=144789>

Goodin, D. (2017). Virtual machine escape fetches $105,000 at Pwn20wn hacking contest. Hack worked by stitching together three separate exploits. Retrieved April 28, 2017, from <https://arstechnica.com/security/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/>

IBM. (2017). Benefits of cloud computing. Retrieved May 8, 2017, from <https://www.ibm.com/cloud-computing/learn-more/benefits-of-cloud-computing/>

Infosec Institute. (2012). Virtualization Security. Retrieved April 29, 2017, from <http://resources.infosecinstitute.com/virtualization-security-2/#gref>

JDEE1Tips. (2015). JDE003 – JD Edwards Release History. Retrieved April 10, 2017, from <https://www.jdee1tips.com/single-post/2015/12/30/JDE003-JD-Edwards-Release-History>

Lin, F. & Shih, T.(2010). Cloud Computing: The Emerging Computing Technology. Retrieved May 08, 2017, from <http://www.ijicic.org/elb10-0515.pdf>

Microsoft. (2009). Changes in Functionality from Windows Server 2003 with SP1 to Windows Server 2008. Retrieved April 07, 2017, from <https://technet.microsoft.com/en-us/library/cc753208(v=ws.10).aspx>

Microsoft. (2016). Failover Clustering in Windows Server 2016. Retrieved April 07, 2017, from <https://docs.microsoft.com/en-us/windows-server/failover-clustering/failover-clustering-overview>

Microsoft. (2010). Hyper-V: Avoid using snapshots on a virtual machine that runs a server workload in a production environment. Retrieved April 30, 2017, from <https://technet.microsoft.com/en-us/library/ee941140(v=ws.10).aspx>

Microsoft. (2016). Plan for Hyper-V Security in Windows Server 2016. Retrieved April 30, 2017, from <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/plan-for-hyper-v-security-in-windows-server-2016>

Microsoft. (2016). Windows Server 2016. Retrieved April 11, 2017, from <https://www.microsoft.com/en-us/cloud-platform/windows-server>

NEC. (n.d.). Virtualization and Consolidation Solutions – Features and Advantages. Retrieved May 9, 2017, from <http://www.nec.com/en/global/solutions/servervirtualization/merit.html>

NIST. (2015). NIST Big Data Interoperability Framework: *Volume 5, Architectures White Paper Survey*. Retrieved May 9, 2017, from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-5.pdf>

NIST. (2012). Guide for Conducting Risk Assessments. NIST Special Publication 800-30, Revision 1. U.S. Department of Commerce. Washington, DC. Retrieved April 28, 2017, from <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

NIST. (2011). The NIST Definition of Cloud Computing. Retrieved May 9, 2017, from <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Oracle. (2017). Engineered Systems Documentation. Retrieved May 9, 2017, from <https://docs.oracle.com/en/engineered-systems/>

Oracle. (2016). Oracle Managed Cloud Services. Retrieved April 30, 2017, from <http://my.oracle.com/site/cloud/index.html>

Oracle. (2017). JD Edwards EnterpriseOne Tools System Overview Guide. Retrieved April 12, 2017, from <http://docs.oracle.com/cd/E61420_01/doc.92/e64056/toc.htm>

Rapid7. (2017). Vulnerability & Exploit Database. Retrieved April 30, 2017, from <https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0109>

SAS. (2017). Big Data - What it is and why it matters. Retrieved May 9, 2017, from <https://www.sas.com/en_us/insights/big-data/what-is-big-data.html#dmtechnical>

Smartbridge. (2017). The Benefits of Upgrading JD Edwards. Retrieved April 08, 2017, from <https://jdeupgrade.com/why-upgrade/benefits-of-upgrading-jd-edwards/>

Stallings, W. (2014). Operating Systems: Internals and Design Principles. Upper Saddle River, New Jersey: Pearson Education.

Tanenbaum, A. & Bos, H. (2015). Modern Operating Systems (Global Edition/4th Edition). Upper Saddle River, New Jersey: Pearson Education.

VirtualizationAdmin.com. (2008). What is a snapshot? Retrieved April 28, 2017, from <http://www.virtualizationadmin.com/faq/snapshot.html>