Analysis of a Secure Virtual Desktop Infrastructure System

Yijie Tong

A thesis submitted to Auckland University of Technology in partial fulfillment of the requirements for the degree of Master of Computer and Mathematical Sciences (MCIS)

2015

School of Computer and Mathematical Sciences

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Signature: _____ Date: _____

Acknowledgement

This research work was completed as part of Master in Computer and Information Sciences (MCIS) course at the School of Computer and Mathematical Sciences (SCMS) in Faculty of Design and Creative Technologies (DCT) of the Auckland University of Technology (AUT), New Zealand. I would like to thank my family for their support throughout my entire MCIS study. The entire school of the AUT has also provided great assistance in my study. I would also like to thank in particular all teachers, supervisors and administration at AUT.

I would like to show appreciation to the guidance and support that my supervisor Dr. Wei Qi Yan has offered. I would also like to say thanks to my secondary supervisor Dr. Jian Yu and our school administrators for their support and guidance throughout the MCIS.

Finally I would like to thank my MCIS peers for their great help in the past two years.

Yijie Tong

Auckland, New Zealand

January 2015

Abstract

With an increasing number of personal computers introduced in schools, enterprises and other large organizations, workloads of system administrators have been on the rise, due to the issues related to energy costs, IT expenses, PC replacement expenditures, data storage capacity, and information security. However, application virtualization has been proved as a successful cost-effective solution to solve these problems. In this thesis, the analytics of a Virtual Desktop Infrastructure (VDI) system will be taken into consideration for a campus network. In this thesis, previous developed system is going to be justified and the relevant improvements will also be presented. Besides, the rationales for these improvements are to be introduced.

This project conducts four research work associated with a college's new VDI system. (1) Requirement analysis and design of the VDI system. Throughout the thesis, general demand of the college, functional requirements of the VDI system and performance requirements of the VDI system will be introduced. After that, the VDI system will be divided into four modules, namely client-side module, application management module, system resource management module and user data management module. (2) The implementation of the VDI system. The college's network topology, network configuration, virtual machine installation and applications installation will be implemented in this thesis. Also, this thesis will present the optimized resource allocation of the VDI server by using quantitative calculation rules of the physical servers' consolidation. (3) Reliability and usability of the VDI system. Our investigations associated with the reliability problems in a virtualization infrastructure will be committed. This thesis will emphasize the reliability of the Physical to Virtualization (P2V) method in a virtualization processing. (4) Testing. A functional testing, a capability testing and a performance testing will be completed before end of this thesis. After the testing, an optimal result will be given as the outcome.

Keywords: intelligent network, application virtualization, VDI, App-V, security, vSphere, Xen Desktop

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Backgrounds and Motivation

A vast majority of system administrators have a large number of tedious tasks, for example, regular updating software and anti-virus feature database, installing patches of different Operating Systems (OS). All of these workloads make system administration error-prone, inefficient, tedious and time-consuming. Even if there were only a few failures when the system administrator installs patches, it would leave the security to the hidden danger.

Virtual Desktop Infrastructure (VDI) is a very effectively solution to solve this kind of problem. VDI can offer a flexible desktop service by managing and delivering applications, so as to provide enterprises significant benefit as follows (Herrod, 2006).

- Save the cost.
- Reduce registry and system bloat on user's PC.
- Simplify software deployment.
- Centralize software updates.
- Simplify OS deployment.

In related work, a project about the VDI system for the L-College will be introduced. The L-College is one of the largest evangelical schools in New Zealand. The main tertiary courses of the L-College are related to pastoral, biblical, historical, teaching and technological subjects. Currently, the college has more than 1,100 students.
The Auckland campus of the L-College is located at Waitakere city.

There were several critical contributions in the previous Microsoft Application Virtualization (App-V) VDI project. Compared to those traditional application virtualizations, the project offered a high flexible system. Flexible virtualization makes virtual applications work more like traditionally installed applications, which allow local and virtual applications to communicate and enable control of the virtual applications so as to share environments. Different from VDI products, there is no dedicated drive letters required. It is easy for IT professionals to work with and take

action on App-V diagnostic information because App-V logs Windows events into different files and categories. Compared to traditional VDI solutions, one of the most important feature of cloud-based application virtualization is web-based management, which makes it easy for IT professionals to get their work carried out while getting away from their desks. But the disadvantage of the cloud-based VDI solution is that they have to find a cloud service provider, which is going to increase the cost. In the previous project, although there is no cloud service, we still can provide the functionality of web-based management (Golden, 2008).

Moreover, different from the previous work in App-V VDI system and other normal campus VDI systems, this thesis offers three kinds of access models.

- In the first access model, all of the virtual applications are supported by Xen Desktop and Xen App, an individual operating system image is created by the View Manager. In this way, there is no need to create a physical operating system for each client. This image is able to generate Virtual Operating Systems (VOS). Once a client has been authenticated by View Manager, the Xen Desktop will combine the VOS with the customer's authorized virtual applications and their configuration files so as to create another integrated personal virtual system (Williams, 2007).
- The second access model is similar to an environment of the working station without disk. This model is designed for certain staff's PCs, which have not a hard disk, those PCs can be boot up from the network card by using Pre-boot Execution

  Environment (PXE), then communicate with VMware vSphere through the View Manager server (Jang, Choi & Kim, 2013).
- The third access model is suitable for the sub-sector and mobile staff. Those users access the View Manager through the WAN for authentication. Once a user has been authenticated, he can get the authorized virtual applications. All of those virtual applications are stored in an application server cluster (Beaty, Kochut &

Shaikh, 2009).

1.2 Objectives of the Thesis

The objective of this thesis is to allow IT professionals' easy installation and management of software on the L-College computers in a high-security environment. Two clear and accurate findings will be justified in this thesis,

- Design and development of a VDI system for the L-College to overcome the problems existing in their networks:
  1. In L-College, they do not have enough computers for all of the students, so the L-College encourages students bring their own computers to the class. On another hand, most of staff and students in L-College prefer to use their own smart device for working or studying, such as their personal laptop, smartphone and smart tablet. But, once private data of L-College has been spread across those different personal devices, how to keep the data secure and how to make sure all of users are able to access the data from different devices has become problems.
  2. Also, there are more than 300 campus computers in L-College's offices and computer labs; to manage those computers is a really tedious job, which has been discussed in the part 1.1. To reduce the workload of IT technicians is also a huge challenge.
- Make sure the stability of this VDI system in the convention processing of physical to virtual (P2V).

  In this thesis, P2V conversion has been used in two aspects, in which physical server is converted into virtual server, and run Windows applications on other platforms, such as Macintosh. The stability in the P2V convention processing is very important, which will have an effect on the security and performance of the VDI system.

1.3 Structure of the Thesis

The whole thesis has been divided into three parts. The first part introduces the concept and the main technology, which has been used in the VDI. The second part illustrates the methodology of how to design an VDI system with different functional modules in a specific network environment. The last part depicts the testing, analysis, discussions and conclusion of the thesis.

In Chapter 2, different kinds of VDI methods have been introduced, which include Centralized Virtual Desktop, Secure Local Virtual Desktop Images and Presentation Virtualization. The key products of the VDI have been introduced as well, such as App-V, XenApp and ThinApp.

Chapter 3 explains the research methodology of this thesis. A systematic design and implementation procedure is also described in this chapter.

Chapter 4 details the final testing results and main outcomes. The section explains the testing experimental setup and analysis of the tests conducted on the simulation environment. Outcomes of the testing experiments are detailed with figures. At the end of this chapter, complete analysis and discussions are carried out for the outcomes and results.

In Chapter 5, the conclusion of this thesis will be drawn and future work will be addressed.

Chapter 2 Literature Review

2.1 The Methods of the VDI

Generally speaking, there are three kinds of VDI methods, Centralized Virtual Desktop, Secure Local Virtual Desktop Images and Presentation Virtualization. Each of them has its own features and infrastructure, before a VDI system would be conducted, we ought to choose the VDI method carefully.

Table 2.1 Comparisons of three types of VDI

	Centralized management of virtual desktops	Support for consumerism scenarios	Users must maintain a constant network connection	User experience needs to meet traditional PC expectations
Centralized Virtual Desktop	√	√	×	×
Secure Local Virtual Desktop Images	√	×	×	√
Presentation Virtualization	×	×	×	√

2.1.1 Centralized Virtual Desktop

As for the first type of VDI, all of the application images should be matched with an Application Virtualization Server and when an application virtualization client requests the application from client's PC. It is streamed to an independent environment on the client's computer for execution. The application will start running since it has got enough data to support it running. Normally, there will be no conflicts between this application and the others since they are isolated from each other. This kind of application virtualization is well known as centralized virtual desktop.

When application virtualization clients log in to a server, the server can issue different clients their own exclusion permissions according to the corporate directories such as AD, in this way, the permissions to download software by clients can be restricted. This also supports the function of centralized management and deployment of a single image (Liao, Jin, Hu, & Liu, 2010). Once the software has been matched and used, the software's preferred settings and profiles would be saved in the clients' cache memory to ensure that the clients are able to access those software when they are off line. Any service patches and updates of the software are applied to the application virtualization server image and when the clients match the software next time, they could choose to update the software and get the newer version (Yan, 2011). If clients are not sure about the newer version of the software compatibility to their OS, clients could revert back to the older version, but the condition is that the older version is still retained on the application virtualization server. In this way, there is a list of available software for the client, who exists as a Graphical User Interface (GUI) based window on the clients' computers, and the clients are able to match and run any software from the list anytime (Huber, Quast, Hauck & Kounev, 2011).

2.1.2 Secure Local Virtual Desktop Images

In the second type of the Application Virtualization, the software is loaded as an image from the application virtualization server remotely, and the software runs in the application virtualization servers. In this way, the only thing that is sent over the LAN is the remote display screen information, which is required to be seen on the clients' computers. This type of application virtualization is more like the desktop virtualization, the difference is in the desktop virtualization both of software and operating system, but hereinafter only the software is virtualized (Yu et al., 2013). This kind of application virtualization is well known as secure local virtual desktop images.

The most significant advantage of the second type of the application virtualization is that it does not matter what kind of Operating System (OS) is in the clients' machines for executing the software as they are being run in the server. Another advantage about this type of application virtualization is it is more suitable for mobile devices, like mobile phones and iPads, as these mobile devices do not have enough processing power to run processor hungry applications, but a powerful server does (Hung, & Min, 2010).

2.1.3 Presentation Virtualization

The third type of the application virtualization is presentation virtualization, which represents a category of virtualization technology that abstracts the processing of an application from the delivery of its graphics and I/O. With the application installed in a single location, presentation virtualization enables its use by multiple, simultaneous users. Each user connects to an individual session stops a server supporting presentation virtualization. Within that session, there are the applications that have been provisioned for the user. In the presentation virtualization, the applications are running on a remote computer, however, the User Interface are transmitted over the network to the thin machine from the server (Sharma, Shenoy, Sahu & Shaikh, 2011).

2.2 The Applications Status of the VDI

Application virtualization separates the app from the OS, allowing IT technicians to deliver applications in the most efficient way. These are just a few of the other benefits, we don't have to install apps. They are easier to patch and upgrade. And we have the opportunity to run multiple versions on the same OS. Plus, in the age of bringing our personal device, application streaming allows IT to deliver apps to many kinds of endpoints. In today’s market, the three largest VDI products venders are VMware, Citrix and Microsoft.

All of Citrix, Microsoft and VMware are taking very similar methods on the topic of desktop virtualization. Meanwhile, each vendor offers its own hypervisor, on which the virtualized desktop hosted (Wohrmann et al., 2012).

2.2.1 VDI from Microsoft

App-V provides centralized management, so admins can limit users' access to certain apps. Microsoft's application virtualization tool is popular in shops moving to Windows 7 or 8 because it lets users interact with virtualized Windows apps, such as Office. The latest version, App-V 5.0, reduces disk requirements by allowing IT to turn off local application storage. Moreover, it has enhanced application diagnostics and monitoring. The latest version of App-V provides a more native application experience to users. IT technicians can also deploy and track apps through Microsoft Silverlight, which means they can access their admin console via the Internet. For mobile workers, App-V 5.0 allows applications to stream over a WAN using Direct Access, and it is also integrated in Windows To Go.

Hyper-V is a hybrid hypervisor, which is a virtualization toll installed on an OS. But during installation it has redesigned the OS architecture, and consequently it looks just like a next layer on the physical hardware.

In Hyper-V, there are couple components; the most important two are Hyper-V Manager and Hyper-V Server. By using the former, IT technicians are able to create, modify and delete virtual machines; configure virtual networking and proceed other additional dependent manipulated.

Hyper-V Server is a compact edition of Windows Server where all of the functions which are irrelevant to virtualization have been deleted, so as to make the server as small as possible. On another hand, due to the fact that fewer components mean less patching, Hyper-V Server requires less maintenance time and it is more secure (Carbone & Larson, 2009).

Generally speaking, Microsoft Hyper-V is a server virtualization solution, and App-V is an application virtualization platform.

2.2.2 VDI from VMware

ThinApp is an application virtualization tool provided by VMware. In some aspects, ThinApp has some functions that are not offered by App-V and XenApp. For example, ThinApp is able to deliver applications in an offline environment, and it is much more portable than other application virtualization tools. We run ThinApp applications from almost everywhere due to the feature of that users do not have to install any drivers or software. In addition, they don't need administration permissions to access applications from remote locations, such as an airport lounge. Still, some administrators complain that the VMware ThinApp is more cumbersome to deploy. It's also trickier to manage applications because it doesn't come with a centralized management platform. If we are experimenting with the cloud and mobility, we should also know that ThinApp 4.7 integrates with VMware's Horizon Application Manager (Ventresco, 2013). The older version, VMware ThinApp 4.6 integrates with View 4.5 and above, but not all administrators need deliver virtualized applications to virtual desktops. There are a large number of things that we need to know about how to license, manage and deploy the ThinApps, particularly if we are using them in a view environment. A new endeavor by VMware, ThinApp Factory automates the application packaging process. This virtual appliance, which plugs into vCenter or VMware Workstation, takes the encoding and distribution out of administrators' hands (Lo, 2005).

VMware View is a virtualization product, which enables IT technicians to isolate a desktop from a physical device or location, and then deliver the desktop as a managed service from a centralized location (Guo, 2012).

For both VMware View and XenDesktop, connections to virtual machines are managed by a server that acts as a connection broker. Although the basic architectural components are the same for the two virtual desktop infrastructure (VDI) systems, Citrix and VMware support their hypervisors differently. VMware View is designed to work with Elastic Sky X (ESX) and/or Elastic Sky X integrated (ESXi) servers.

Furthermore, these servers must be a part of a vCenter server. Citrix, on the other hand, is much more flexible. Citrix has its own hypervisor, XenServer, but XenDesktop can alternatively be run on vSphere or even on Microsoft's Hyper-V (Dittner & Rule, 2011).

2.2.3 VDI from Citrix

The application virtualization solution produced by Citrix is XenApp. Different with ThinApp and App-V, XenApp provides not only application virtualization, but also an application delivery system. Citrix Streaming, a part of the Citrix virtualization tool, can get a license for XenApp or XenDesktop (Hwang et al., 2008).

XenApp is pretty confined to its server environment or a client environment, making it difficult to port around. Still, Citrix added support for Microsoft App-V in XenApp 6.0. At Citrix Synergy 2012, the company combined XenApp with its desktop virtualization product, XenDesktop, into the Excalibur offering. XenApp is useful for IT shops that have a wide variety of applications - old and new - and want to virtualize apps with Citrix Streaming that ThinApp and App-V don't support. Citrix XenApp 6.5 reduces application launch times through the Instant App Access feature. Improvements to the HDX protocol also allow apps to run in higher-latency environments. Plus, XenApp 6.5 includes a Mobility Pack that improves application delivery to mobile devices (Yu, Cao, Wen & Lu, 2006).

Citrix XenDesktop is a desktop virtualization system that centralizes and delivers Microsoft Windows XP, 7 or Vista virtual desktops to users at anywhere. Virtual Desktops are dynamically assembled on demand, providing users with pristine, yet personalized desktops each time when they log on. This ensures that performance never degrades, while the high speed delivery protocol provides unparalleled responsiveness over any network. Citrix HDX delivers a high definition user experience for virtual desktops and offers the best performance over any network connection. The open architecture of XenDesktop offers choice and flexibility of virtualization platform and user device. Unlike other desktop virtualization

alternatives, XenDesktop simplifies desktop management by using a single image to deliver personalized desktops for users and enables administrators to manage service at levels with built-in desktop performance monitoring. Citrix FlexCast delivery technology enables us to deliver every type of virtual desktop, hosted or local, physical or virtual, each specifically tailored to meet the performance, security and flexibility requirements of each individual user (James, 2010).

Chapter 3 Research Methods

3.1 Related Studies

There are a variety of methods having been used to create a virtual desktop system. Baratto et al. have proposed a mobile virtual desktop computing hosting infrastructure (MobiDesk). In a MobiDesk system, there is a thin virtualization layer, which is used to extract users' application stream from a specific client terminal, and transfer the processing of all of the applications to the server logically. Another in MobiDesk is a virtualization layer. This layer enables users to take application resources from the server by executing the selected application and deploying the virtual desktop on users' hardware. The MobiDesk system is a cluster system with a proxy server. Figure 3.1 shows the architecture of the MobiDesk system which encompasses a proxy server, couple session servers, a network file system (NFS), a storage server, and a number of display devices (Baratto, Potter, Su, & Nieh, 2004).

Figure 3. 1 MobiDesk architecture

Calder et al have also proposed a technique: Entropia DCGrid (Desktop Distributed Computing Grid). In this solution, there are two functional modules to support this system: 1) a desktop controller and 2) a sandbox execution layer. The desktop controller in this system is used to manage the executions of applications, charge the resources assigned to clients and hide the identifications of the users. Another functional module is a lightweight Sandbox Execution Layer to convey and virtualize a response from the system. This functional module can protect the virtual desktop and applications from some of the attacks. The sandbox execution layer is developed by both of a device driver and a dynamic binary interception (Greamo & Ghosh, 2011).

There are three layers in the server side of this Entropia DCGrid system. From the bottom to the top, they are physical node management layer, resource scheduling layer and job management layer. The physical node management layer is used to manage the connection and communication between the clients and server. The resource-scheduling layer is used to match the request and schedule the process between server and client. The job management layer is used to manage the mass of request and files of clients, and then transfer them to the resource-scheduling layer (Calder, Chien, Wang & Yang, 2005).

For those organizations that have employees dialing in from remote locations, access to the main data center is one area where security design is very crucial. This covers both the connection for users into the data center, as well as protects the data center against attacks from endpoints that are not managed by the enterprise and have been infected in some ways (Sailer & Jaeger, 2005). For the user coming into the network, either an IPSec or SSL VPN will be required to protect the connection between the endpoint and the firewall. Any traffic between the virtual machine session and the endpoint will be on a remote protocol, of which there are many to be chosen from. As far as choosing SSL or IPSec VPNs is concerned, which of these is required by the organization will depend on whether we expect to have VPN client software installed on the user's endpoint device, and the cost for licenses involved. The part between the VPN and the central data center is the next stage to protect. For organizations that wish another layer of security, they could put a demilitarized zone (DMZ) in place and proxy the user across, so that the central data center is not in direct contact with the user connected in (Janssen, 2010).

One more issue to consider when looking at VDI and security is patching. Because VDI enables us to run either persistent images created from scratch or a mixture of both, there can be some problems in patching and making sure that images are up to date. However, the amount of time cost on this is far less than that of encountered when we have to visit each physical machine in order to commit updates. The first step in the process for updating virtual machine images is to apply the patch to the

master image, once the update has undergone through the necessary testing and approvals procedures. For organizations that are running non-persistent images, this means that all the virtual machines based on this central image will automatically be up to date before they are restarted next time. With persistent virtual machine images, the patch management process will be more difficult. Once a virtual machine image has been created from the master image, it will develop a lifecycle of its own deployment when it comes to update. Patches installed after deployment, or in general any changes to overall make-up of the virtual machine image applied to the deployed virtual machine will be lost after the next round of deployment (Janssen, 2010).

The method also affects how to backups of a desktop virtual machine are taken. The most common approach is for the virtual machine to be snapshotted. An image is taken at a particular point in time. If the production image is damaged or corrupted, then the backup image will be quickly restarted. However, any changes or patches applied since the snapshot has been taken will be lost (Janssen, 2010). Taken this into consideration, it is important to check the status of a virtual machine whether the right patches have been applied. This process is based on recognizing that certain changes are missing from the newly deployed virtual machine, and then the required changes (e.g. patches) can automatically be re-applied or a prompt received on whether these changes should be reinstalled. This process ensures that standardized images like desktop virtual machines will always be up-to-date without having to rebuild the image completely each time, or manually check that patches are installed and updates have been applied.

3.2 Research Methodology

According to the issues existing in the campus network of the L-College, some research methodologies have been designed to indicate how to design this application virtualization system. The main purpose of this chapter is to identify the potential research problem, describe the potential virtualization methods, software tools and storage solutions.

In this thesis, design science is selected as a research methodology. Design science is one of the IT research methodologies, its focus is on developing a new system or evaluating the performance of the designed system. Because it concentrates on the process, it has a significant impact on this thesis, evaluations and quality assurance of this project. According to the design science, an IT project is divided into six parts: problems giving, requirement analysis, solution design, solution development, testing and evaluations (Peffers et al., 2007).

The analysis stage is one of the fundamental steps of this thesis. After requirement analysis, the thesis comes up to the design stage. In the design, the analysis outcomes will be imported as the cornerstone of design in performance and security aspects. The objective of the design stage is to find out the appropriate methods, tools and technologies; no matter it exists already or not. Once the design phase is over, the thesis will move forward to the development phase. In the step, all of the selected methods from the design phase will be implemented. The output of this step will be a finished VDI system, which needs to be tested and evaluated. In this testing step, it contains a performance evaluation and a security evaluation.

At beginning of the design and implementation of a new solution, the IT environment of the L-College must be analyzed in every details. In order to figure out the L-College's environment and get ready for designing the VDI system, the follow key points should be taken into consideration: user data, personalization, application management, and hardware management. The results from analyzing these four aspects may lead to the successful selection of the methods and technologies (Hoffmann, Schumann, Maksoud & Premier, 2010).

In the aspect of user data, we need identify what the current situation of the L-College's corporate data, localized documents, and application preference are. All of those may be observed by the staff in charge or use of a profile management method. In a VDI system, the user data may directly influence the flexibility and mobility of this system, so analyzing and determining the location and the way for storing and accessing data are extremely critical in design of the VDI system. In the aspect of personalization, the main component we need to analyze is the application preferences for clients settings (Ainsbury, Hussein, Hinnant & Lahham, 2000). Computer skill of users is one of considerable factors for analyzing in design time. Some vendors of the VDI solutions like Citrix, who promoted VDI products at various levels for the customers with different computer skills. A high quality end product may have more functions, but it is hard to use it for the customers with lower computer skills, and vice versa. Therefore, it is necessary to make out the computer skills of those potential users, which can be obtained possibly by a survey via questionnaires (Hoffmann, Schumann, Maksoud & Premier, 2010).

In application management, which applications will be virtualized is an important issue to the performance and security state of the VDI system. The other similar questions include which specific applications are used most often, how many needs to be virtualized. In order to obtain those answers, a survey needs to be conducted, a questionnaire need to be well designed and deliver to the potential users of the VDI system. The questionnaire will ask those users to list ten most frequently used applications. Application management includes not only which applications are in use, but also what is the way they are be used, what the data requirements for this application are, whether there are any applications that can interact with a specific application, and so on. The outcomes of the application management will be used to calculate the workload of applications, identify the workloads of those applications, all of all, the quality and quantity of this thesis within the given timeframe (Bolte, Sievers, Birkenheuer, Niehorster, & Brinkmann, 2010).

The results of the application management also will be used to identify the process of application delivery in the VDI system. There are typical question related to this process, such as, whether the specific application is able to running on our chosen Operating System, whether the specific applications should be installed directly in a client machine or streamed on server, whether it is possible that an application package is to be delivered, what could bind several applications together, and whether the specific required application can work in an offline environment or not (Ranganathan & Foster, 2002).

Device and hardware management may focus on the problems associated with the device and the hardware of the L-College. The question may include whether the users of this VDI system would like to use pads or smart phone devices, laptops, multiple monitors, kiosks or a combination of them, find out which types of devices are widely used in the VDI system. This may be very helpful for selecting the delivery technology as well as the hardware management, the number of laptops, the parameters of the clients and the bandwidth of the campus network are also critical for the VDI system. All of the information can be obtained from a survey and an interview with the IT department of the L-College.

Determining the business use case is also very important in the system, data will become useful till it is transferred to useful information. The items discussed in preparing for VDI part, which may help a researcher to collect the raw data for designing the VDI system. Then this part may lead a researcher to transfer that raw data into information. Different organizations or companies always have a different business use case, especially in a scope and in details. However, for the sake of simplicity, the use case determination is used to logically collect users and applications, and each case may have its unique usage needs and unique delivery needs.

For a VDI system, the target users, user's devices type, access methods, applications needs and delivery method need to be defined in each case. Before designing this VDI system, we should consider almost all of potential requirements;

due to the VDI system is not easy for modifying or updating. That is why experienced technicians always suggest us design the VDI system with as much flexibility as possible.

Another benefit from business use case determination is that, it groups the users of the VDI system and sets the priority level for those user groups. This may help to develop the VDI system in most phases, like design phase and further management. For instance, if marketing user group is the first use case targeted for this VDI deployment in the L-College, then the applications and delivery requirements for that

use case may obtain the desired priority (Yan, 2011).

3.3 Previous Work

3.3.1 Virtualization Methods Selecting

According to the three kinds of the VDI methods introduced in the Chapter 2, which is more suitable for the L-College's case and also to meet the desktop requirements? A decision tree can help us to find out which one or combination matches with those all requirements, as shown in Figure 4.1(Williams, 2007).

If the organization strongly hopes to run shared applications, the presentation virtualization method is a good solution. On the other hand, the disadvantages associated with this method include the user environments that cannot be isolated; also, presentation virtualization may affect performance of the OS.

Centralized Virtual Desktop is another method, which is able to centralize and protect the data; it is also able to isolate application environments (Martin, 2008). By using this decision tree method, we eventually chose the VDI as the virtualization method for this thesis.

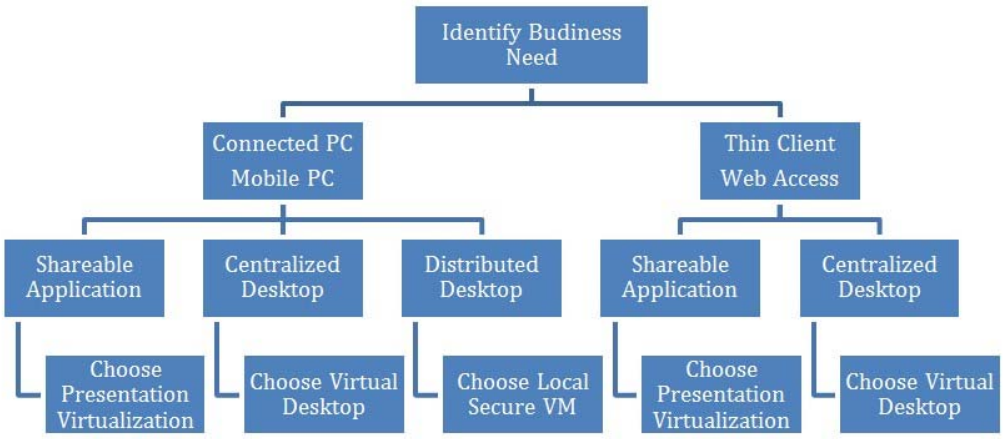

Figure 3.2 Decision tree for virtual software choosing.

After comparing these three kinds of application virtualization, we conclude that the Centralized Virtual Desktop of the VDI is more suitable for the L-College's virtualization desktop infrastructure, there are three reasons.

In the L-College's case, the advantages of using the Secure Local Virtual Desktop Images (the software are run from a centralized server) cannot be shown very well. Firstly, in the L-College, 90 percent of the students' PCs and all of the school's PCs are based on Windows Operating System, so they don't need to care other OSs, e.g. Mac and Linux. If the college has to support other OSs, they may use Hyper-V to solve this problem easily. Secondly, the L-College just requires that clients should be able to match Microsoft Office from the application virtualization server and this is not a processor hungry application, so most of the mobile devices have enough processing power to support this. (Jin & Miyazawa, 2002)

In the L-College, there are more than 1000 students and staff, so if half of them want to use the application virtualization system simultaneously, it will cause overload on the application virtualization server if the Secure Local Virtual Desktop Images are used. However the Centralized Virtual Desktop (the software is streamed from a central server and run in clients' computers) could do that, because in this way, lots of clients' computers will process the workload instead of a single server. Another advantage of the Centralized Virtual Desktop is that it has the ability to run different versions of the same software on the same client's computer, like
Office2007 and Office2010 (Back, Park, Yang, Song & Jeong, 2013).

3.3.2 Storage Solution Selecting

Storage solution is another issue we have to take into consideration. For a VDI system, the storage solutions may need to be selected from three aspects as follows. The first aspect is storage arrays, nowadays, the three most popular storage arrays for the VDI are SAN (storage area networks), DAS (direct-attached storage) and NAS (network-attached storage).

The second aspect is storage protocols; the options may include NFS (Network

File System) and FCoE (Fiber Channel over Ethernet).

The third aspect is the drive type, which may include SAS hard disk, SATA hard disk and SSD hard disk.

Rob Commines has presented a method how to select the VDI storage solutions for a VDI system, which need meet the following four requirements.

- This storage solution is aware what the needs are for the applications from the storage platform.
- This storage is able to backup and recovery through snapshots and replication of virtual machine images (Sindoori, Pallavi & Abinaya, 2013).
- This storage solution contains Data De-Duplication function.
- This storage solution is extensible and scalable.

After analyzed a testing, the final solution has been chosen is SATA hard disk with NFS and direct-attached storage (DAS).

3.3.3 Software Tool Selecting

Except the structure method and storage solution, picking up the right software tools is very important for designing and developing this VDI system as well. Due to the fact that we have chosen the Centralized Virtual Desktop as the structure method, the results from the literature review show that, the VDI software methods which is able to be used to support the Centralized Virtual Desktop includes Citrix XenApp, VMware ThinApp and Microsoft App-V. For choosing the right one, we employ a pre-deployment testing to compare the following matrices and a better solution.

From the matrix, it is easy to see that, Microsoft's App-V is the best solution for the L-College's Application Virtualization Infrastructure. Compared to Citrix's XenApp and VMware's ThinApp, the App-V not only has the best compatibility, which is also more economical, the only shortcoming is the aspect of execution overhead (Kant, 2009).

In the App-V, there are three parts are included. The first part is the Application Virtualization Management Server, which is used to publish its applications to clients. Applications that have been sequenced are imported into the server for publication to clients that have the desktop client installed and configured to communicate with the server.

Table 3.1 Comparisons of different VDI products

	Microsoft App-V	**Citrix XenApp**	**VMware ThinApp**
Support 64-bit OS deployments	√		√
Support 64-bit applications	√		
Support 32-bit applications	√	√	√
Support 16-bit applications	√		√
Central point for application license management	√	√	
Reporting the Virtualization applications usages	√	√	
Low cost of implementation	√		
Quick up and running			√
Easy for packing an application	√		

The second one is Application Virtualization Client, which is the component that actually runs the virtual applications. The Application Virtualization Client enables users to interact with icons and double-click file types to start a virtual application. It also handles the streaming of application content from a streaming server, and then caches it before starting the application. The application content is structured so that all the content need to start the application, and handling initial user

interaction is streamed to the end user machine first. There are two different types of Application

Virtualization Client software: the Application Virtualization Client for Remote Desktop Services (formerly Terminal Services), which is used on Remote Desktop Session Host (RD Session Host) server systems, and the Application Virtualization Desktop Client, which is used for all other computers. Before running the setup, Microsoft C++ 2005 SP1 and 2008 SP1 Redistributable Packages and Microsoft Application Error Reporting need to be installed first.

The last one is the Sequencer. In this thesis, the App-V Sequencer has been installed on a virtual Windows 7, which is on the same physical computer with App-V management server. This virtual OS is created by Hyper-V. Sequencing, which is the process used by Application Virtualization to create virtual applications and application packages, requires the use of a computer with the Application Virtualization Sequencer software installed. In the process of sequencing, the Sequencer is launched in a monitor mode, and then the applications to be sequenced are installed on the sequencing server. Next, the sequenced applications are started, and its most important and commonly used functions are executed so that the monitoring process is able to configure the primary feature block. The primary feature block contains the minimum content in an application package, which is necessary for running an application. Once these steps are completed, the monitoring mode will be stopped, also the sequenced application will be saved and tested to verify the correct operation (Hannifin, D., 2010).

3.3.4 Functional Testing

After the App-V VDI research project has been done, a functional testing has been conducted.

Table 3.2 Functional testing results

TEST	**CONDITION**	**ACTION**	**EXPECTED SATISFACTORY RESULT**	**TEST RESULT**
Publish software from App-v management server to client Publish Microsoft Office 2007 to Student Group and Staff Group Publish ITunes to Staff Group	Publish Excel2007 and iTunes	Login as a Student account	Can find Excel on client's desktop	Pass
		Login as a Staff account	Can find Excel and ITunes on client's desktop	Pass
		Login as a Visitor account	No published software	Pass
	Move Excel2007 from the management server and add	Login as a Student account	Can find Word on client's desktop	Pass
		Login as a Staff account	Can find Word and ITunes on client's desktop	Pass

	Word2007 in	Login as a Visitor account	No published software	Pass

3.4 Novelty of This Thesis

After the evaluations of the previous work, this thesis got a tremendous improvement on the aspects of framework design, functional design, security solution and especially key technology. The main components of this new VDI system include Citrix XenDestop, which is used to manage the system server cluster and support the interaction between the VDI system and the clients; VMware View Composer, which is taken to manage the data storage in the system; and VMware View Manager, which is in use to support the access authentication and manage the system image (Villanueva & Cook, 2005).

This new VDI system is using Citrix XenDesktop to achieve the interaction between the VDI system and the clients, XenDesktop is able to collect the request from the client and send a response back to the client. Clients can login to the View Manager through the RDP protocol or PC over IP protocol by using Cirtrix XenDesktop or Web browser, then the client is able to view one or more virtual machines which have been authorized to be accessed (Barham et al., 2003).

3.4.1 VDI System Design

 Overall System Framework Design

The client software of desktop virtualization system of the L-College is accessible to the server in enabling the corresponding applications running on the server; the called data on the server and the generated application data are stored on the server; the interfaces of the running applications return back to the client. According to the specific needs of desktop virtualization system for the L-College, the overall framework of desktop virtualization system of the L-College is shown in Figure 3.3.

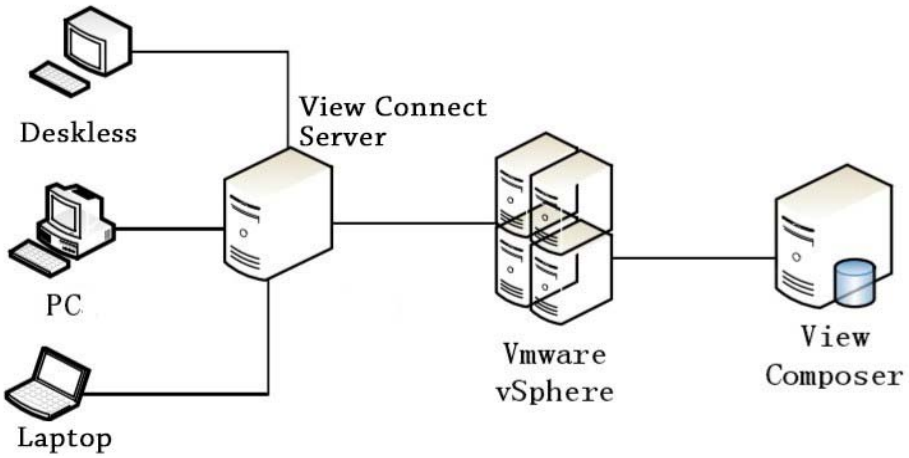

Figure 3.3 Overall framework

The desktop virtualization system of the L-College is divided into four modules, which include client, view connection server, servers and data storage. The client side uses XenDesktop 4.1; View connection server runs the View Manager to manage the user connections and system mirror; the server side adopts VMware vSphere4; the system data storage optimization is achieved by

VMware View Composer (Nishikiori, 2011).

- System Function Module Design

If we overview the overall infrastructure of this system, it is mainly divided into the following modules, which include VMware vSphere module in managing the server cluster, ViewManager module in controlling the user access and load balance, View Composer module in realizing data storage optimization, XenDesktop module in interacting with users, offline desktop module in disconnecting to the server and the reinforced display module in enhancing the user experience. The system function modules are shown as the Figure 3.4.

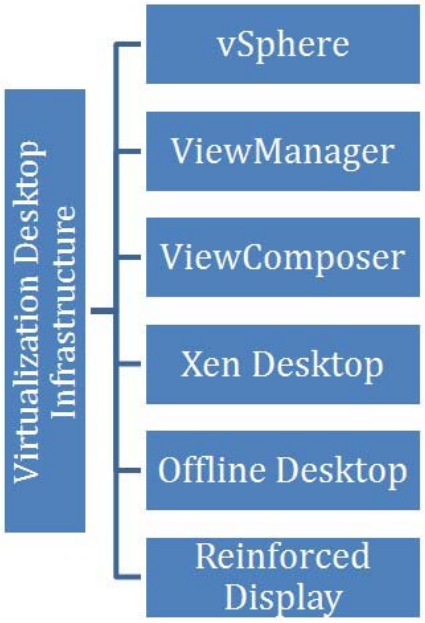

Figure 3.4 Functional modules

- Overall System Scheme Design

The overall application virtualization system schemes are shown as the Figure 3.5.

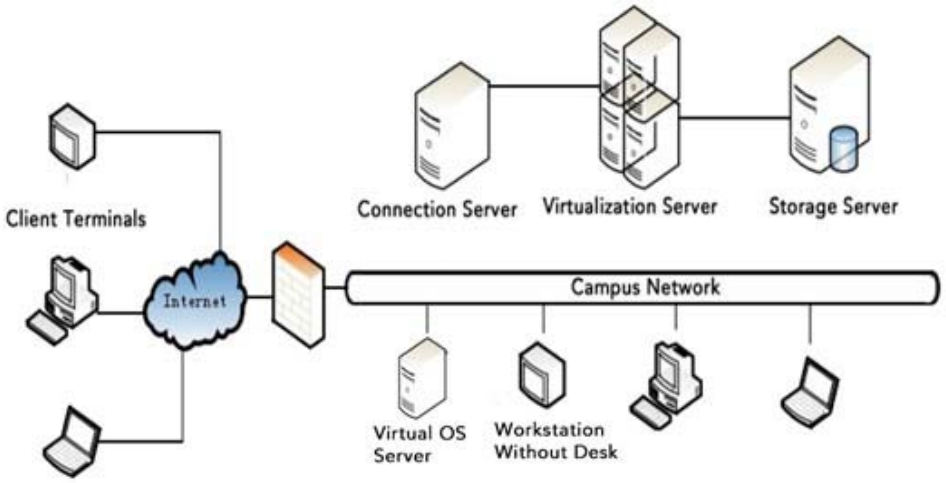

Figure 3.5 The system architecture

From the Figure 3.5, the application virtualization system has offered three kinds of different connect services by using the LAN in the server room, campus LAN and the Internet.

- Single Mirroring Virtual Desktop Based on the Intranet Standard Tasks

The standard virtual desktop and application are based on XenDesktop

and XenApp on the background. The View Manager is used to generate a single mirroring operating system. When many users are in need, it is possible to generate the standard operating system in batch by virtue of mirror image. Afterwards, it is just required to separately manage and maintain the mirror. As long as the operations like the system and patch upgrades are just being run in this mirror, it is able to complete all the updates for the users. In this way, it is able to save a lot of storage space in avoiding to build a physical operating system for each user. When the office staff has a direct access to the unified authentication platform of View Manager, XenDesktop makes the free and dynamic portfolio of the operating systems generated by mirror image, the virtual applications delivered by View Manager and the individual configuration files in a dynamic and on-demand way so as to provide a complete virtual desktop for the users. The users acquire the authorized virtual desktop and virtual applications in carrying out the daily office work. The user data is intensively stored in the file server. The operating experience is just as the same as the experience in the local system (Man & Kayashima, 2011).

- Local Fluidized Diskless Desktop of Graphic Design based on the Intranet

  The teaching and administrative staff uses the diskless PC, boot the communication of View Manager server and VMware vSphere through the network card PXE, acquire the storage location of the virtual hard disk and create the diskless workstation environment. The mirror image of operating system is stored on VMware vSphere. The software and patch updates are undertaken on the server for one time. The local fluidized desktop will recover the standard status upon the rebooting at each turn. 3D and other graphical designs are implemented upon the guarantee of the desktop performance, the complete utilization of the local hardware resources as well as the maximized use of the original hardware resources (O'doherty, 2012).

- Access to the Remote User Application Based on the Extranet

The sub-sector or mobile workers are able to access the unified authentication platform of View Manager via WAN. The authenticated users are available to receive the

authorized virtual applications of which these applications are intensively deployed in the VMware vSphere server cluster, and the user data are intensively stored in the backstage file server (Lowe, 2011).

The desktop virtualization solutions of the L-College are based on the computing server architecture. The front-end device is just used to display the interface without the support of the powerful hardware resources. Even for the eliminated PCs, they can easily run WinVista, Windows 7 and the other mainstream operating systems.

3.4.2 Client Side Module

- Client Access Method

  The desktop virtualization system of the L-College mainly applies the Citrix XenDesktop tool to realize the system interaction with the users. The main function is to collect the user requests and give a feedback of the processing system results on the user requests.

The first method is View Client. The client applies the Citrix client XenDesktop program to log in to View Manager through the RDP protocol or PC Over IP protocol of which we can check one or more permissible virtual machines. Citrix XenDesktop provides a complete and unmodified desktop environment that is compatible with the traditional or customized applications and delivers the corresponding customized desktop as required by each user. With the support of a wide range of clients, the users are accessible to log in to their own desktop at any time through a variety of the virtual desktop equipment and the local printer, USB devices or other peripheral units. In addition, the redirection of multimedia improves the end-user experience on the rich multimedia (Kouril & Lambertova, 2010).

The second method is Internet Browser.The client applies IE or other browsers to log in to View Manager through the RDP protocol or PC Over IP protocol of which we can check one or more permissible virtual machines. VMware View provides the complete and

unmodified desktop environment that is compatible with the traditional or customized applications and delivers the corresponding customized desktop as required by each user (Grossman, 2009).

The third method is WAN environment. Since all the computation tasks are intensively stored in the physical data center servers, within the local area network (LAN), the users can not perceive the clear speed differences among the virtual desktop and the local computer on account of the relatively small delay, especially in the case of the applied RDP protocol. Within the WAN environment, the user is likely to complain about the loading speed of virtual desktop due to the unequal delays that the network delay reaches more than 30 ms. Therefore, in the WAN environment, it is recommended to use Citrix XenDesktop under the PC Over IP protocol. Even though the network delay reaches up to 200 ~ 300 ms in the WAN environment, there is a good performance in meeting the requirements of the client applications at the different levels (Mell & Grace, 2009).

- Desktop Virtualization

Citrix XenDesktop is available to deliver the end-to-end desktop solution to generate the virtual desktops as required dynamically. Upon the user login, the user can receive a personalized new desktop in ensuring the maintenance of the desktop performance. Based on the high-speed delivery agreement, XenDesktop is able to offer the unparalleled response speed under any network condition. In terms of the IT organizations, XenDesktop is accessible to respectively deliver the desktop operating system, application and user settings, greatly simplifying the management of desktop lifecycle and significantly reducing the cost of ownership.

Citrix XenDesktop is able to deliver the desktop as required at anywhere. Meanwhile, the life cycle management is significantly simplified. It is able to provide an end-to-end desktop solution in speeding up the delivery of desktop for the end users and a more powerful data protection and monitoring. And the

cost will be decreased by more than 40% (Sotomayor, Montero, Llorente & Foster, 2009).

The desktop virtualization technology is applied for the centralized management of data center in easily achieving safety protection and backup. However, there still exist the issues of the same life cycle management. The IT department still needs to manage, maintain and update the mirror image, the installed applications and user settings for each virtual desktop. In addition, the implementation of desktop virtualization also brings new challenges. In particular, the network performance is greatly reduced, and the storage cost of the desktop mirror network is significantly increased for each user (Mousa, 2012).

- Application Virtualization

Ctrix XenDeaktop isolates the application from the basic layer of the operating system, which is able to tremendously enhance compatibility and make the management job much easier. The packaged application generated by View Manager is able to run on the data server of the virtualized applications, it also could be accessed by the shortcut on the virtualization desktop, in this way, volume of the desktop image could be greatly reduced. Because the isolation and virtualization of the applications, the clients of the Citrix XenDesktop is able to run multiple applications or different versions of one application, of course, there will be no conflict (Miller & Pegah, 2007). Those virtualized applications will be centralized via management and deployment; consequently we make sure the applications the users used is the latest version.

3.4.3 Application Management Module

In the L-College's application virtualization system, the View Manager has been used to support the application management server. The main function of the View Manager includes clients' access control and virtual application image management. VMware

View is a manager of the virtual desktop, which has been installed on a Windows Server 2008, then the VMware View Manager is able to work with Microsoft Active Directory, hence the virtual application will be assigned to the different AD client group according to their permission by using WEB management interface. This makes sure the security of the data, which is only accessed by a limited group. By using Cirtrix XenDesktop interface; users are able to access personalized virtual desktop in a VMware vSphere environment, Windows Terminal server environment or remote PC within a secure way. At the other side, system administrators control, monitor and audit the desktop activities, also manage the loading balance of multiple Windows Terminal Server (Velte & Velte, 2009).

One of features of the View Manager is the centralized management. Based on View Manager, it is accessible to make the centralized management and maintenance for the desktop in time and resources saving for the college. More and more colleges will replace the traditional PCs with the virtual desktop that is running in the data center server, and deploy the desktop from a single location. The advantage is that the users have an access to their desktop at anywhere as well as their personalized desktop environment which is called myView. The centralized management and support desktop are available to improve the flexibility, shorten the response time and reduce the operating costs. In terms of the centralized deployment model based on View Manager, the applications of the college are just deployed in the data center. Since the clients and the servers are located in the same Local Area Network (LAN), the application performance and security are improved so that the users easily have the access to the data center through any terminal and any network. The college just needs to manage the data center within the local area network (LAN) so as to simplify the management and maintenance. It is possible to install and configure the application software on the server side to greatly simplify the configuration and deployment of the office environment (Basak, Toshniwal, Maskalik &Sequeira, 2010).

Another feature of the View Manager that has been used in this thesis is remote access control. All of the Remote Desktop Protocol (RDP) between the clients and View Manager Connection Server is protected by using View Manager Connection Server,

View Manager Client and View Manager Web Access. All of those protocols will be encapsulated by View Manager (Such as the RDP within HTTPS), it includes below advantages.

- RDP creates a tunnel by HTTPS, and encrypts it by using SSL
- It is a very powerful security protocol; it is at the same security level with the online banking service.
- Just one HTTPS connection is able to support all of the communications between the client and the server.
- Multiple desktop connections are able to use this HTTPS at the same time, which will reduce the cost.
- View Manager controls the two sides of the HTTPS connection, and then the reliability of the underlying protocol will be increased.
- If the internet connection is interrupted, once it reconnects, the system will recreate a new HTTPS connection and RDP connection, the users do not need to re-login
- The access mechanism of View Manager uses stranded Web protocol; thus, remote users are able to access the View Manager by proxy server. If in the deploy environment only having View Manager Connection Server, the HTTPS secure connection will stop in the View Manager Connection Server. In the DMZ deploy environment, the HTTPS secure connection will stop in the View Manager Security Server. If users hope to direct the RDP communication from the client to the virtualized desktop, administrators will disable the secure connection for the View Manager Connection server (Martin, 2008).

Firstly, users need to be authenticated, View Managers support multiple ways to undertake the authentication, which include two-factor authentications and fingerprint authentication. After the users have been authenticated, the administrator is able to access users' account information, and check which applications are able to be accessed by those users (Zhang, Juels, Reiter & Ristenpart, 2012).

When the client uses one virtual application or access on virtual desktop, they use the virtualization server and password management by View Management, in this way, the

clients log in and finish the application calls in seconds. After that step, clients use the applications just like in the local computer.

The system administers cannot only set the accessible permissions of the applications for the configured users, but also record the access log of the each client.

The access permission of the virtual applications are strictly controlled by the View Manager, the operations have been managed strictly including Copy/Past, print, save to local and port access (Scarfone, 2011).

View Manager also contains the integration function of the virtual desktop pool management. Based on the control mechanisms of vCenter, it is possible to deploy and manage the virtual desktops. The View Manager provides the following desktop types. Single Desktop

In terms of the desktop virtualization system of the L-College, a single desktop refers to a single virtual machine in containing Citrix XenDesktop achieving the remote access via the View Manager client. A user who has the permission to use the desktop will always have an access to the same system upon the connection each time. The single desktop is suitable for those users who need the exclusive desktop. Meanwhile, it is also applicable for the multiple users to have an access to the installed application that has a high cost with the license of a single machine at a different time periods.

- Automatic Desktop Pool

The automated desktop pool contains one or more dynamically generated desktops. Based on the VirtualCenter virtual machine templates, these desktops are automatically created and customized by View Manager. This type of a desktop pool includes Permanent Desktop Pool and Impermanent Desktop Pool. Permanent Desktop Pool refers to the assignment of an exclusive desktop in keeping all the session documents, applications and settings for the user. This kind of the desktop is statically assigned upon the user connection for the first time. Afterwards, it can be applied for all the subsequent sessions. Impermanent Desktop Pool means that the users connect to the different desktops upon the connections at every turn. There is no permanent environment and user data in the sessions (Borough, Kochut & Beaty, 2007).

- Manual Desktop Pool

The manual desktop pool refers that the administrators of the View Manager manually build the virtual machine pool. This kind of a desktop pool also can be classified as Permanent Desktop Pool and Impermanent Desktop Pool.

- Terminal Service Pool

Terminal service pool refers to the desktop resource pool of the terminal services (TS) offered by one or more Windows terminal servers. The multiple desktops will be delivered at the same time in terms of a terminal service desktop resource.

In order to meet the requirements of high availability and high scalability, the multiple View Manager Connection Servers are deployed. The first deployed View Manager Connection Server is installed as the standard version instance (this option is available during the installation process). In this case, it installs a new instance of the LDAP directory while the View Manager Connection Server is in support of all the functions of its local LDAP directory. In order to extend this environment, the second server is installed as the copied instance. (Ruest & Ruest, 2009)

During the installation process, the users refer to the existing View Manager Connection Server while the copied instance will join the standard versions in forming a View Manager Connection Server group. In the standard edition instance, the configuration data of LDAP View Manager is duplicated to the copied instance. The bi-directional replication protocol is established between two servers. Once the configuration of View Manager is changed in one server, it will be immediately reflected in another server automatically (Hwang & Wood, 2012).

Both of the servers are functioned in the same way. Once a server fails, another server continues running the system separately. After the failed server recovers to a normal state, the modified configuration data of the LDAP View Manager is reflected on the server. Both of the servers will be updated to the latest version at the same time. In this group, it is available to add a third server or the additional View Manager Connection Servers. The additional copy instances will be installed. During the installation process of the copied instance, the user is able to refer to any existing group member so that the new server will be added into the group. Upon the

completion of the installation, there will be no differences for the copied instance and the standard version instance. If the first standard edition instance is invalid, it is possible to add the other copies by referring to the active View Manager Connection Server. All the configuration data of View Manager is backed up by the backup LDAP directory instance.

3.4.4 System Resource Management Module

VMware vSphere is mainly applied to implement the management of hardware and software in the server cluster, namely achieving the joint management on the server cluster of the central machine room. Therefore, the server cluster is devised as the super computer with a powerful CPU processing power and a huge storage capacity.

The desktop virtualization system of the L-College is constructed on the VMware vSphere. VMware vSphere is allowed to independently run the multiple virtual desktops for users and share the underlying physical hardware resources such as CPU, network connection and memory. Under this architecture, the users are separated from each other so that each user has his operating system. At the same time, it is feasible to implement the accurate resource allocation and prevent the collapse of the applications and the failure of the operating system that are caused by the other users (Beloglazow & Buyya, 2010).

All the servers are deployed with the VMware vSphere virtualization architecture software. Each server with two-socket quad-core processor or two-socket six-core processor can bear the workload of an average of 30 to 50 users (Shamma er al., 2011). The specific loading capacity depends on the performance of the applications. Each physical server is equipped with eight network cards. The functionalities of eight cards are functioned as Service Console management, online migration (VMotion), IPSAN connection, the communication of a virtual machine and the physical network. Under the redundancy for each other, a high availability of network card is achieved through the VMware built-in NIC TEAMING, which includes the network link failover and load balancing of network card (Feng, Tang, Luo, & Jin, 2011); (Murphy, 2001). 1000M of connection speed shall be required for the network cards in the communication of VMotion and the physical network. All the files on the virtual machine are stored in IPSAN for all the users. On the basis of the HA (High

Availability), FT (Fault Tolerance), VMotion (online migration) and DRS (Dynamic Resource Scheduling), the backup and disaster recovery protection are available to the desktop applications. At the same time, the machine halt is fully eliminated due to the planned server maintenance, such as a physical server (Beloglazow, Abawajy & Buyya,
2012).

3.4.5 User Data Management Module

In the desktop virtualization system of the L-College, the data management is mainly achieved by the VMware View Composer technology. The personal data of the teachers and students is stored on the server side. As well, it needs to guarantee that the unauthorized users will not steal the personal data, namely it is unwarrantable to access the other's data for the users. Therefore, it is necessary to implement the functions for the data on the server side, which includes the isolation of data storage, data storage protection and data protection, etc.

- Isolated Storage

In the L-College's VDI system, VMware View Composer has been installed in a Windows Server 2008 OS, every AD user has its own disk space by choosing NTFS and Windows Server user Profile. All of those disk spaces, working directory and temporary files are secretly managed and limited, such as avoiding cross access between users (Ranganathan & Foster, 2002).

- Data Protection

Under the traditional pattern, the applications are distributed on all the clients for the college. The security considerations are involved into each link: server, client and end-to-end network; the system maintenance and security management are involved with the terminal equipment and the wide area network (WAN) segment for the college. With the direct access to the background via the client, the transmission data is the authentic application data for the college of which the data will be cached in the local devices or intercepted in the transit. All of these elements are unsafe; While the user has an access to VMware View Composer Server, the incremental change information and the mouse

keyboard change information are transmitted in the screen. In the client, there is no cached application data in the local device (Principato, 2010). Compared to the direct captures of the office data, it is much more difficult to deduce the real office operations and data. Therefore, it is said that data is always stored in the safest place. The biggest benefit of VMware View Composer is to prevent the lost data at any time by using the application virtualization method. For the remote user who has an access to the intranet from the public network, the security permission of VMware View Composer is controlled by the strict user authentication. Because the client's keyboard, mouse action and the refreshing parts of the display interface are just transmitted in the network, the office data and codes are not downloaded into the local client; information like data, cache and cookies is controlled in the central confinement environment; in addition, ICA protocol also contains a variety of encryption technology in ensuring the secure data transmission in the display interface and user operations. Although the operation in the client is just like the operation in the local machine, it is not allowed to implement the modification, backup, copy, printing and the other operations without the consent of the authority. Through the release way of the applications, the internal staff and external staff from the cooperative colleges are only allowed to use the corresponding applications without the access to open the other applications or data information (Bazargan, Yeun & Zemerly, 2011).

Based on the working principle of the diskless workstation, the client adopts the diskless PCs. The office environment for the staff is achieved through the diskless booting of VMware Provisioning Server. All the data is stored in the file server. The setting to disable all the local ports (such as USB port, print port, etc.) ensures that the core data is not leaked.

- Storage Optimization

VMware View Composer uses the linked clone technology that is permissible to quickly create the desktop mirror from the master image in achieving the rapid deployment of virtual machines in batch. Whenever the updates are available in the main image, it is able to implement the updates in the virtual desktops in a few minutes, greatly simplify the deployment and maintenance, and reduce the operation cost. In this

process, the user settings, data or applications are not affected. Therefore, the users still use the working desktop in an efficient way. Even if when the application is undergoing the changes, it is still working in an unaffected way (Ranadive, 2012). (Nong & Fang, 2012)

3.4.6 Resource Allocation of the Virtualization Server

In an ideal situation, according to the advice from the Citrix, the overall CPU requirement, overall memory requirement, overall network I/O requirement and overall disk I/O requirement of the VDI server need to follow a set of the calculation formulas, which is a difficult thing to achieve in a real-world environment. So, in practice the ideal formulas need to be modified. Firstly, we will talk about the ideal calculation formulas. (Das, Padala, Padmanabhan, Ramjee & Shin, 2010)

The resources requirement of the Virtualization Server

The overall CPU requirement of the server is calculated by,

$$\sum \quad * \quad * \qquad (3.1)$$

where stands for the number of the CPU kernel, refers to the speed of the CPU who's unite is MHz, represents the percentage usage of the CPU.

The overall memory requirement of the server is calculated by,

$$\sum \quad * \quad 32 \qquad (3.2)$$

where refers to the total memory in MB; means the percentage usage of the memory.

The overall network I/O requirement of the server is calculated by,

$$\sum \ \sum \quad _ \quad _ \qquad (3.3)$$

where _ stands for the average Bytes received per second; _ symbolizes the average Bytes sent per second.

The overall disk I/O requirement of the server is calculated by,

$$\sum \quad _ \quad _ \qquad (3.4)$$

where _ is the average Bytes read per second; _ shows the average

Bytes wrote per second.

- **The physical resources can be provided to each packaged applications** The CPU resources provided to the virtual applications from the physical server is calculated by,

$$* \quad \_ \quad 1 \quad * 85\% \qquad (3.5)$$

where is the total number of the CPU; _ is the number of the kernel in each CPU.

The memory resources provided to the virtual applications from the physical server is calculated by,

$$2 \qquad (3.6)$$

where stands for the total number of the memory who's unites is GB (Waldspurger, 2002).

The desk I/O capability provided to the virtual applications from the physical server is calculated by,

$$\_ \quad \_ \quad 85\% \qquad (3.7)$$

The network I/O capability is provided to the virtual applications from the physical server calculated by,

$$\_ \quad \_ \quad 85\% \qquad (3.8)$$

- **The number of the packaged applications can be supported**

The number of the packaged applications provided by the physical server is calculated by,

$$/ \qquad (3.9)$$

where is the resources (e.g. CPU, memory, disk I/O or network I/O) can be provided by the server; is the resources that are required by the virtual applications. The values of for CPU, memory, disk I/O and network I/O
need to be calculated separately, the minimum value out of the four will be chosen as the number of the packaged applications.

All of the above formulas are ideal formulas, which is used to purchase the virtualization server. According to the information collected by Performance Monitor,

after analyzed, the ideal one is modified as the follows (Urgaonkar, Kozat, Igarashi, & Neely, 2010).

The number of the Kernel of the CPU provided to the virtual applications from the physical server is calculated by,

$$* \quad * \quad / \qquad (3.10)$$

where is the total number of the kernel of the physical server**;** is the maximum utilization rate of the CPU. stands for the rated speed of the CPU for each virtual application, which in the units of MHz ≈0.8 (Kalyvianaki, Charalambous & Hand, 2009).

The memory provided to the virtual applications from the physical server is calculated by,

$$\sum \qquad \min \qquad (3.11)$$

The network I/O provided to the virtual applications from the physical server is calculated by (Almeida et al., 2010),

$$\text{Net} \quad \text{Max Byte} \qquad \text{1024} \qquad (3.12)$$

3.4.7 Hardware Configuration and Network Topology

In the L-College's campus network, all of the user management system, resource management system and application management system are located at the center server, staff and students use the application virtualization service by connecting to the server through the campus network.

In this campus network, the storage LAN connects to the servers through switch NO.2, and the users of the VA system are able to access the servers through switch NO.1. Host 1-5 connect to the VMware Sphere server through Switch 1 by using double-link. In this way, the system still is running normally even if there is one link fails. For the server hosts in the Figure 3.6, all of the parameters are calculated by the modified euqation from the Chapter 3.4.6.

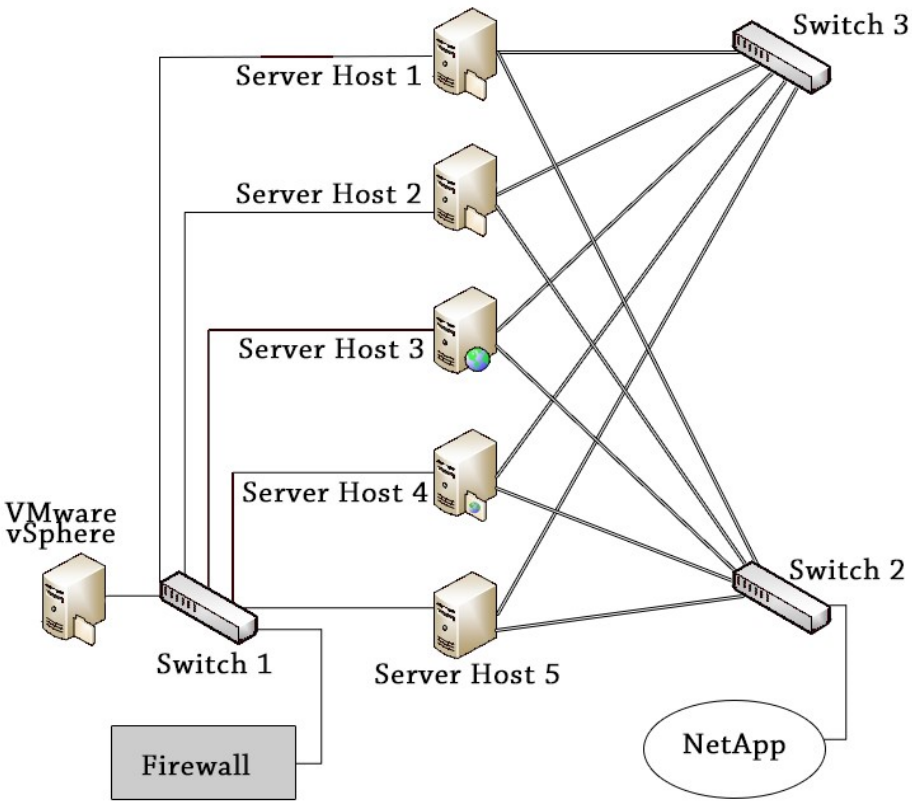

Figure 3.6 Topology of the L-College

In the L-College's application virtualization system, WMware vShpere management server is used to manage five host servers. All of these six server machine use the same hardware parameter, which as shown in the table 3.3.

Table 3.3 Server parameters

Item	**Detailed Parameter**
CPU	Intel Xeon CPU X5560@ 2.8GHz 2.8GHz×8=22.4GHz
RAM	4G×8=32G DDR3 1600
Network Card	Broadcom NetXtreme Gigabit Ethernet
Hard Disk	1Tb

In the VA system, the server stores all of the data in the L-College's storage system through the optical network. The storage solution has been used is NetApp FAS2050 system, which is a stable ischia/ FC SAN/ NAS storage application with up to 104TB capacity. The parameters of the NetApp FAS2050 are shown in the table (Alvarez, 2011).

Table 3.4 Storage NetApp FA2050 parameters

Item	**Detailed Parameter**
Management Software	Data on tap
Management Method	Snap Mirror/ Snap Restore/ Snap Shot
Supported Application	Snap Manager/ Snap Driver/ ischia
Hard Disk	50TB expandable
File Share	NAS

In the L-College's application virtualization system, the IP address, subnet, IP of the gateway and the swathes need to be managed and assigned, which is shown as the table 3.5.

Table 3.5 Networking parameters

Item	**Switch**	**Gateway**	**Network Segment**
Storage Network	NO.3	192.168.2.1 To 192.168.2.24	192.168.2.1 To 192.168.2.255
Campus VPN	NO.2	192.168.1.1 To 192.168.1.24	192.168.1.1 To 192.168.1.255

Outgoing Network	NO.1	122.57.60.1 To 122.57.60.24	122.57.60.1 To 122.57.60.255

3.4.8 Installation of the Virtual Machine

In this system, the applications which need to be installed on the servers for managing the virtual machine include follows.

- VMware VCenter Server 4.0

VMware Vcenter Server is installed on the outgoing server, which is used to manage the hardware and software resources on that five host servers. In this way, the users will see those five independent host servers as one super server. Also, the VMware VCenter Server is able to manage the loading balance of those hose servers.

- ESX 4.0

Those five host servers are able to communicate with the outgoing server by installed the ESX. Thus, the outgoing server manages the hardware resources of those hosting servers (Haletky, 2007).

- View Manager

The View Manager is installed on the outgoing server, which is used to manage the requests from users. On another hand, there will be multiple VM images generated by the VMware VCenter Server to supply the virtualization desktop service to the users.

- Data on tap is used to manage the storage system.

By installing that virtual machine management, there is a super computer with 112 GHz process capability, 160G RAM and 50TB storage capability. This super virtual machine is created and managed by VMware sphere. And this super virtual machine is able to create multiple personalize virtual machine images for users by View Manager (Mashtizadeh, Celebi, Garfinkel, & Cai, 2011).

3.4.9 Security Methods

The application virtualization system helps schools or companies to integrate their IT resources, reduce workload and time. But the security problems associated with application virtualization haven't been got enough attentions as much as it deserved. In 2011, a survey of "Information Week" magazine shows that more than 70% of large companies own one or more than one virtual server (Arwidmark & Nystrm, 2011). Unfortunately, only 17% of them have deployed different levels of security solutions for their VDI system. Among the companies who do not have any security solutions, almost half of them agree with that there is no difference of security solutions between virtual server and traditional server, while another 18% of them said that they did not know whether the Application virtualization system changed the security rules (Padala et al., 2007).

There is no doubt that the application virtualization technology has affected and even changed the structure of the traditional system and data storage. On the other hand, it has created a large number of new requirements associated with information security in a virtual environment. Most of the relevant research work shows, the commonest way to enhance the security of the VDI system is to increase the security of each individual component in their system, including servers, clients, storages, sequencers, etc (Dasilva, Liu, Bessis, & Zhan, 2012). In order to enhance the security, the governance of companies encourages e a "one server, one application" policy. This is in order to reduce the possibility of an attacker using a flaw in either the host or applications to take control of the server.

For the security in the Microsoft Windows, because the VMware vSphere environment is based on the Windows authentication methods, thus, the users' privilege is the most important key of the system's security. For this VDI system, we create an Organizational Unit (OU) on the domain controller, and only give the basic permission to the users in the OU. By using the group policy hide drive, those users are able to write and read their personal document on the server by using login script. All of the personal documents are only allowed to be saved on this catalogue. (Sahoo, Mohapatra, & Lath, 2010)

Every Active Directory domain contains a standard set of OUs and containers that are created during the installation of Active Directory. These include the follows. (Sands, Hsieh, Hendricks, & Williams, 2012)

- Domain container, which serves as the root container to the hierarchy.
- Built-in container, which holds the default service administrator accounts.
- Users container, which is the default location for new user accounts and groups created in the domain.
- Computers container, which is the default location for new computer accounts created in the domain.
- Domain Controllers OU, which is the default location for the computer accounts for domain controllers computer accounts.

Also installing the antivirus software on the VMware vSphere server is included so as to ensure that virus will not infect the server.

For the security in VMware vSphere, we use VMware vSphere controller to manage the user access permissions and the local equipment permission, such as hard drive, CD drive and printer. Some users in the system are not allowed to use the local drive, when they login to the VMware vSphere with certain applications, they cannot save any documents or data on the local drive (Lowe, 2013).

For the security in networking, the firewall only allows to open port 80 and port 1494. If in future, the Access Gateway has been deployed, and then we need to open the port 443. The ICA protocol of the VMware vSphere is a private protocol, for now, there is not an efficient attack method against ICA. Hereinafter the WLAN environment for the VMware vSphere is relatively safe (Haletky, 2009)

With the application of desktop virtualization technology, one of the major threats to the system is created by multiple VMs' sessions. The migration of running VMs between different servers will reduce the efficiency of network security products to some extent. Original intention of x86 virtualizations is to consolidate the server resources; the idea is that running multiple VMs in a single but powerful server will replace multiple outdated physical servers. Thus, a server session between different VMs will bring an enormous internal traffic. VM sessions between all the

virtualization products are realized through a virtual switch, which allows the server to share all the VMs. External network security tools, such as firewall, intrusion detection, prevention system and abnormal behavior monitor, in theory, cannot detect the traffic existing in the physical server network. While the physical security devices can detect each packet through virtual environment, they cannot see the internal flows. In other words, if a virtual application is infected, it spreads to the whole virtual network; however, physical security equipment at the external will notice nothing about it. To ensure the safety of multiple VMs on the same server, one of the methods is to ensure that VMs are running similar OSs, which has been equipped with effective patches. This means that if the OSs running on one safe server, the sessions between them will be relatively safe. Meanwhile, security products, such as host firewall, must be in place. But there is not inherent security architecture to improve the VDI system; in fact, it also has not proposed such a mechanism to deal with internal security vulnerabilities (Liu & Lai, 2010).

Therefore, it is necessary to establish a new security architecture for an VDI system. Compared to the reasons mentioned above; a better solution we put forward is to use the VLAN (Virtual Local Area Network) technology. VLAN is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration will be carried out through software instead of physically relocating devices. Here, the VLAN we use for the VM is as the same as the one for physical server. If we use VLAN tagging technology, the virtual network can be extended to outside of the virtual environment. Firstly, we give different IP addresses to each VM based on the same architecture; secondly, we use VLAN-based classification method of the network layer, and separate those VMs to different VLANs; thirdly, each VMs cannot communicate directly with other VMs without help of Layer 3 network equipment (Zhang & Zhou, 2009). We create the router on a stick with firewalls instead of routers; then the data exchanges between all VLANs are forwarded in the firewall. In this way, we use the

mechanism of an internal firewall between applications and the VLAN, and then process the data between applications and segment. The firewall and IPS (intrusion prevention system) is directly deployed to a virtual environment. Accordingly, we monitor these internal flows between the virtual machines. We configure all security software (such as passwords, encryption, authentication, auditing, etc.) on the firewall; thereby strengthen the internal security policy; beside firewall records all activities of the VM. A firewall is possibly used to separate a VM from another VM, which can prevent sharing of the serious consequences of the network caused by a single machine. Compared to security issues distributed to all network, centralized security management of firewall is much more economical (Liu & Lai, 2010).

.

3.5 Virtualization Technology of P2V Conversion and Reliability

The virtualization management software of System Center Virtual Machine Manager (VMM) allows the users to turn the existing physical computer into virtual machine during the “physical to virtual (P2V)” conversion process. VMM offers the wizard based on the tasks so as to automatically perform most of the conversion procedures in simplifying the P2V conversion process.

3.5.1 Virtualization Technology of P2V Conversion

The conversion modes are composed of online P2V conversion and offline P2V conversion. The advantage of online conversion is the normal running of the source computer, achieving the real-time migration of “physical machine”. However, a number of servers are conducted through the offline conversion, such as Windows 2000 server system (Asai, 2013).

The characteristics of two conversion ways are stated as below. The characteristics of the online P2V conversion include follows.

- The source computer will be normally run during the conversion process.

- VMM is going to create the local NTFS volume copy and the application program data with the Volume Shadow copy Service (VSS) perceptive function. VMM takes use of the VSS, ensuring the server data backup in the continuous responses of the user requests.
- For most of the physical machine, the default settings of the operating system are online P2V conversion.
- In the whole conversion process, the source computer will be normally operated.

The characteristics of offline P2V conversion include follows.

- During the conversion process, the source computer turns into offline mode
- Upon restarting of the source computer, VMM will clone the volume to VHD upon the entrance of the windows reinstallation environment (Windows). Finally, WMM will restart the source computer and the original operation system is accessible.
- The offline P2V conversion is the only way to convert Windows Server 2000 and reliably transfer FAT volume as well as the recommendation method to transform the domain controller.
- The offline P2V conversion may be the most reliable mean or the unique choice to ensure the data consistency under the certain conditions.

3.5.2 The Research of Disk Space Capacity Allocation and the Integration Service during the P2V Conversion Process

If too much space is allocated from the start, it will cause space waste since the space will not be used up for the users. Based on Xen Desktop, the allocated resources will not be reduced instead the resources are only allowed to be increased. At the same time, too little space will not meet the needs of users. The best practice is to calculate the reasonable allocation value according to the collected performance data prior to the virtualization operations. According to the reference value, it is available to reasonably allocate the smaller disk space. If the distributed space cannot satisfy the

user needs, it is possible to allocate the corresponding resources under the circumstances (Hodgman, 2013).

In terms of Windows 2000 server system, there may arise problems in the P2V integration services. Due to the system environment and other factors, it may lead to the incomplete drivers of the migrated virtual machines in the winServer2000 system. In this way, it is impossible to directly manage the remote connection to the VM. If there appear the similar problems, it is available to login to the hosting server of virtual machines, enter the Xen Desktop management console, and then manually install the Xen Desktop integration services, namely virtual machine driver. Upon the installation, the automatic switch of the mouse shall be confirmed between the virtual machine and the hosting system (Deuby, 2009).

3.5.3 The Research and Application Test of Reliability upon the Virtualization Operation

The enhanced Xen Desktop features are collaborated with a failover cluster so as to promote the high availability of virtual machines under the Windows virtualization environment. Based on the collaboration of the failover cluster and system center virtual Machine Manager, Xen Desktop allows the administrators to interrupt the response of the scheduled halts and respond to the unplanned halts in the shortest possible time.

The following Xen Desktop functions are applied to achieve the highly available virtual machine.

- Failover cluster
- Quick Migration
- Backup

The requirements of high availability of virtual architecture are to ensure the real-time transfer of the cluster nodes. The failover cluster shall be firstly created and managed. Through the Window Server failover cluster, the resources are uniformly planned and managed. During the downtime period, the failover cluster is configured

properly to realize the automatic recovery of virtual machines on the other host (Li, Sun, Zheng, & Shen, 2012, Armbrust et al., 2010).

Xen Desktop is available to transfer the running virtual machines from one physical host system to another. The downtime is reduced to the maximum extent.

Meanwhile the high reliability is also maintained for the management tools of Windows server and System center (Li, Jia, Liu, & Wo, 2013).

The Xen Desktop Live Migration function is able to transfer the running virtual machines from one Xen Desktop host to another. The host cluster configuration supports Live Migration and provides the required basic shared storage management and resource redistribution technology (Michael & Linares, 2011). Xen Desktop is a new characteristic of windows server 2008 R2 while the previous Xen Desktop versions only support Quick Migration. Live migration does not require the network disconnection. In this process, the interruption time is only taken in milliseconds of which the customers almost are not able to detect the difference. Its principle is to use the dynamic I/O redirection function of cluster shared volume (CSV). When there appear the failures between the node A and shared storage, I/O operations are redirected to the node B through the network regarding to the mirror and memory state of shared storage on the node B (Cerling & Buller, 2011).

There are three kinds of Live Migration management methods. Firstly, system center virtual Machine Manager (SCVMM) provides a GUI interface of which it is able to transfer the running virtual machines from the Xen Desktop master server to another master server in the same cluster. If SCVMM is not applied, console of the failover cluster manager (MMC) is to initiate the running virtual machines (Michael & Linares, 2011). When the live migration is achieved from the Xen Desktop master server to another master server in the same cluster, the downtime is shortened to the maximum extent. The Xen Desktop WMI distribution program can also be used to compile the script during the above mentioned Live Migration process. The speed of Live Migration depends on the necessary memory information content and the speed of a shared storage device in the conversion process (Kadupatil, Patil, Shaha, Sarode & Nair, 2013).

Therefore, it needs to install the failover cluster on each node and verify the cluster configuration, build up the cluster, configure the high availability of Xen Desktop (enable the shared volume group, let the virtual machines to be stored on the cluster shared volume of Xen Desktop, configure the high availability of Xen Desktop) and test the Live Migration (Nelson, Lim, & Hutchins, 2005).

The test method is to restart the server on the node 1, simulate its downtime, and observe the running situations of virtual machines. Through the test, it is discovered that the downtime does not affect the continuous business operations when the virtual machine is crashed and all the virtual machines are transferred to node 2.

3.5.4 The Research on the High Availability of Virtual Machines on the Cluster Nodes of Virtual Architecture

In the virtualization architecture, whether the business operations on the virtual machines are affected after the disk space uses up? The corresponding tests are conducted.

Test 1: Whether the virtual machine will be normally operated after the disk space of a single virtual machine runs out?

Test Method: To build two virtual machines with a Win 2003 test and a Win 2008 R2 test. The system disk C: and data application disk E: are filled with data to observe whether the virtual machine will be crashed.

Test Results: When the disk space runs out, the virtual machine is not crashed and normally operated. After the restarting of the machine, it is still normally operated instead it is unable to write data any more. When the space is insufficient, the repeated warnings of the insufficient disk space are automatically displayed in the virtual machine. Therefore, the exhausted disk space of a single virtual machine will not cause any system failure. Adding the disk space or the disks and other disk defragmentation methods in the SCVMM will continue the related business operations.

Test 2: The booting of virtual machines after the entire physical disk space runs out.

Test Goal: To check the booting of virtual machines when the entire physical disk space runs out and the machine is crashed

Test Method: The physical disk space size is set 300G to establish the testing machine, and then copy and append the data until the capacity is exhausted as well as test whether the booting of virtual machine is normal or not.

Test Results: All the virtual machine cannot be started, but the following measures can be taken:

- Delete some files or clean up the disk on the host
- Recommended Practice: About 100M space is reserved on the physical disk space. When a physical disk space will run out, the space is directly deleted to guarantee the normal operation of all the virtual machines. It is a fast and practical method.

3.5.5 Build the Virtual Machines Based on the Operation System Templates

When a new virtual machine is built, the requirements of the user should be satisfied. In the SCVMM library share, all kinds of hard disks and templates are established, such as Win2008R2x64bits, Win2008x64, W2008SP2x86, winZoo3x64, winZoo3x86 and so on. According to the user requirements and practical experience, the CPU, memory and

shall be allocated depends on the version of the operation system.

Chapter 4 Testing and Results

The testing of this project has been divided into functional testing, performance testing and Capability testing. In all of these three tests, black box testing has been adopted according to the following two reasons.

- White box testing cannot identify problems caused by mismatches between the actual requirements or specification and the code as implemented.
- In this thesis, the Microsoft App-V has been employed as the VDI tool, which has been tested by the software engineer of Microsoft by using black box testing method already.

The functional testing of the VMware vSphere system has been conducted first, because the following two tests, performance testing and capability testing only are conducted when the vSphere is working normally. So we can see the functional testing as a preparatory work for other two testing (Agrawal & Nath, 2014).

4.1 Functional Testing of the VMware vSphere System

4.1.1 Test Purposes

This testing is proposed to verify the following functions of the vSphere system; the vSphere system is employed for the deckles machines for the L-College's staff.

- The migration from the physical machine to the virtual machine
- The functions of the virtualization server, storage, and network
- The management, automation and optimization of the VDI
- VMotion
- The high availability of the virtualization server
- Fault tolerance
- Dynamic resource allocation function
- Data Recovery

4.1.2 Testing Environment

Figure 4.1 Topology of the functional testing environment

In order to test the full functions of the VDI system, we need at least two X86 servers, which are used to install VMware's ESX. Each server needs to have at least three 1000 Mbps Ethernet port, which are used for VA network, management network and VMotion network respectively. In order to test the high availability of the virtualization server and vSphere, a shared storage arrays need to be installed, such as the products of SAN, iSCSI or NAS. We also need a Giga bit Ethernet switch and a client machine. The parameters of two ESX servers are as follows.

- *CPU*: Intel 45nm Core 2 Xeon*2
- *RAM*: 8GB
- *Hard desk*: 15K RPM 250GB SAS*2
- *Network Card*: 1GB Network adaptor*2

In order to run the VMware fluently, there is a requirement for the RAM, which is at least 4G, but in this test, we use an 8G RAM in both of two ESX servers. For the CPU, we choose Intel 45nm Core 2 Xeon, it is because in this test, the CPU needs to support Intel-VT and AMD-V technology (Chaudhary, Cha & Walters, 2008); (Younger et al., 2011). The Management Server (VCenter management server) needs to use a single PC, according to the introduction from VMware, the minimum parameters include a CPU with at least 2.0GHz, 2GB RAM. The OS for the Management Server is Windows XP Pro.

4.1.2 Testing Methods and Results

- ESX functional testing

Table 4.1 vSphere ESX functional testing results

Testing Method	Expected Results	Testing Results
NIC Teaming function testing	NIC Teaming is able to achieve network workload balancing and failover capabilities functions.	Achieved
VLAN function testing	Using the logic sub-network to achieve network simplification and network security	Achieved
SAN HBA Multi-path function testing	To achieve the multi-path management of SAN HBA	Achieved
Templates and Clones	Able to create a new virtual machine by using Templates. And able to Clone copy this virtual machine	Achieved
Snapshot	Able to back up and recovery the virtual machine by using Snapshot	Achieved

- High availability of vSphere testing

Table 4.2 vSphereHA testing results

Testing Method	Expected Results	Testing Results
Creating a VMware Cluster	Creating a VMware Cluster successfully	Achieved
Creating a resource pool	Creating a resource pool successfully	Achieved
VMotion	Migrating virtual machines from a host to another by using VMotion	Achieved
Fault Tolerance	If the host of a virtual	Achieved
	machines is damaged, the virtual machine is able to restart on another connected host automatically	
Distributed Resource Scheduler (DRS)	VMware DRS is able to allocate resources dynamically	Achieved
VMware Data Recovery	Able to backup virtual machine centralized by using Data Recovery	Achieved

- VMware Converter testing

Table 4.3 VMware Converter testing results

Testing Method	Expected Results	Testing Results
Install VMware Converter	Install VMware Converter successfully	Achieved
Importing Machines with VMware Converter	Able to import the old server to a virtual environment	Achieved
Boot CD testing	Using the Converter Boot CD for local cold cloning	Achieved
Configuring new virtual machine testing	The old OS on the server is able to run in the new virtual environment after virtualization	Achieved

4.2 Performance Testing of the VDI System

4.2.1 Testing Environment

The topology of the testing environment is shown as the follows.

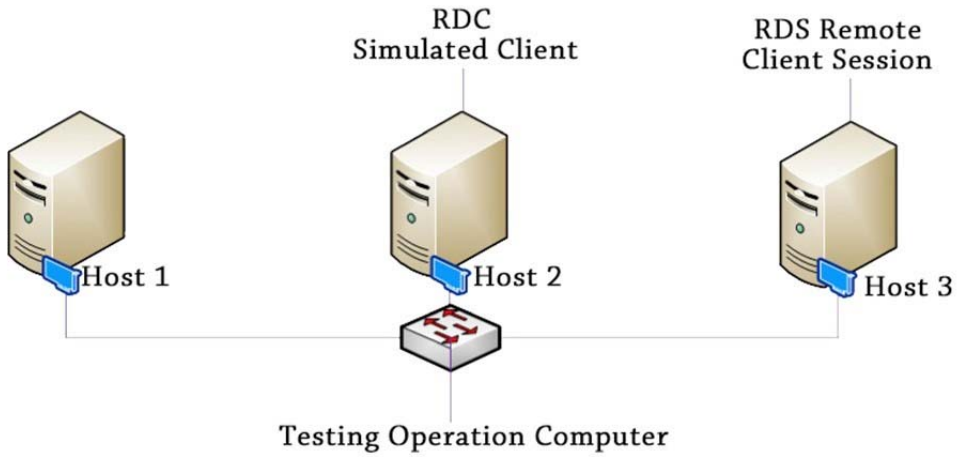

Figure 4.2 Topology of the performance-testing environment

In this testing environment there are three physical servers, the responsibility of each is:

- *HOST 1*: The manage server, which is used to set up the modify the parameter, control and manage the process of the testing

- *HOST 2*: This server is used to simulate the client-ends' actions. This server will connect to the VDI server remotely, to simulate the operation of a remote client.
- *Terminal Session Server*: This is used to undertake the pressure from the remote simulate client, and record the data in the testing.

4.2.2 Testing Methods

Hardware Methods:

In this testing, the parameters of those three servers are same:

- *CPU*: Intel 45nm Core 2 Xeon*2
- *RAM*: 8GB
- *Hard Desk*: 15K RPM 250GB SAS*2
- *Network Card*: 1GB Network adaptor*2

Software Methods:

- The testing environment is built by the below Operating Systems.

  1) Windows 7

  2) Microsoft office 2010/2013
- The testing tool used in this testing is Remote Desktop Load Simulation Tools

Testing Procedure

This testing uses the Windows RDP API to run the pre-settled operations on the clients. In this way it simulates the clients' actions, each RDP simulates one client. Each simulated client undertakes the following actions step by step (Khanna, Beatty, Kar & Kochut, 2006).

- Open Windows Notepad, write 400 words and save as a new document
- Open IE and open three windows not close
- Open Word, type 5000 words around two pages and saves as a new document.
- Open Windows Explore, browse the "My Files"
- Open Excel

In this simulation testing, the client has been set to the higher user experience mode, the parameter of the RDP connection is shown as follows.

- High color 24-bit depth
- 800×600 resolution
- Turn on the function “Font Smoothing”
- Turn on “Menu and Windows Animation”

4.2.3Testing Result

Table 4.4 Performance testing results

	The Number of the Simulated Clients	**Accomplished or Failed**	**User Experience**
Testing1	40	Accomplished	Operation is smooth, no delay
Testing2	70	Accomplished	Operation is smooth, no delay
Testing3	100	Accomplished	The Operation is nearly smooth, there is a little delay when user read and write the file, the delay is < 4 seconds
Testing4	150	Accomplished	The delay is obvious, the delay of the response is > 5 seconds
Testing5	160	Failed	Run out of memory, some clients cannot be connected

4.2.4 Data Analysis

For the performance testing, the tool used is Microsoft Remote Desktop Load Simulation Tools 64 bit. The follows are collected when the client number is 100.

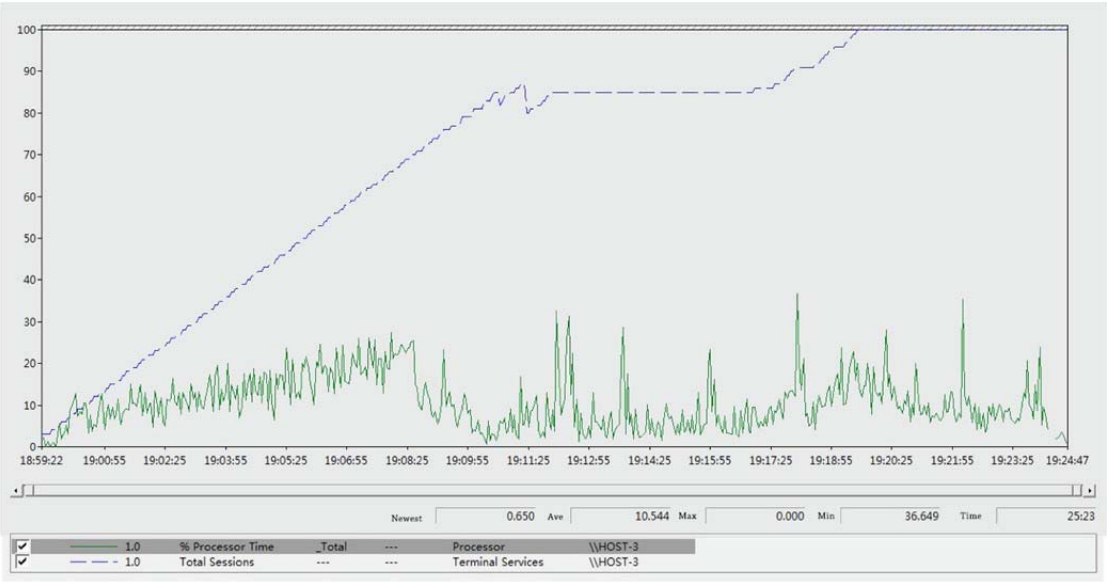

Figure 4.3 CPU processing capability

In Figure 4.3, the blue imaginary line is the total number of the clients being connected to this VDI system; the green solid line is the processor time. This figure shows that, within the whole testing process, the CPU usage rate has never exceeded 30%. This means the processing capability is much stronger.

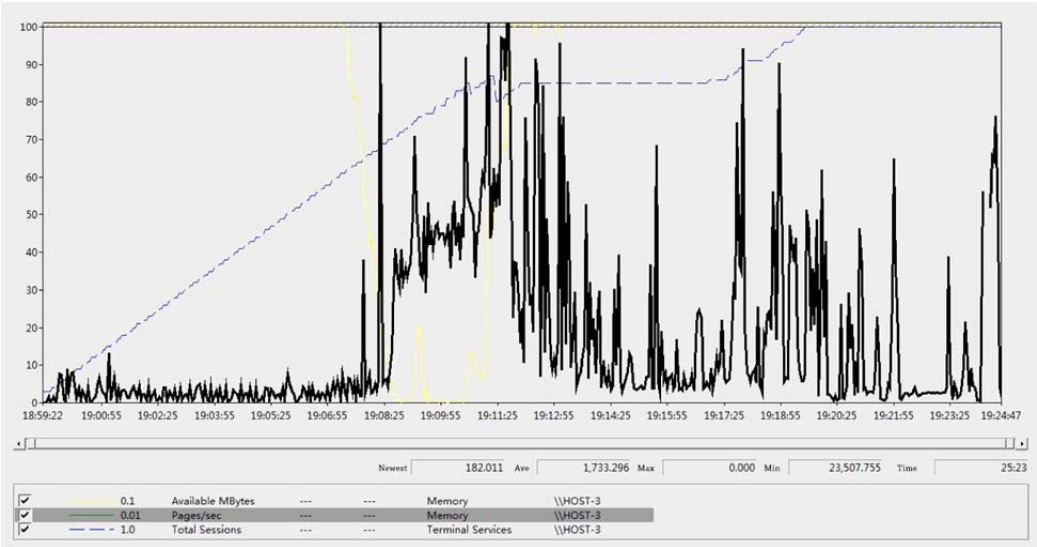

Figure 4.4 RAM usage rate

In Figure 4.3, the blue imaginary line is the total number of the clients being connected to this VDI system; the black solid line is the frequency of pages replacement in memory; the yellow solid line is the available Megabytes in the memory. This figure shows that when the number of the connected client has reached 60, the RAM usage rate substantially increases. When the number of the connected clients keeps increasing, the pages replacements in the memory are becoming more frequently, moreover, some noticeable delay has been occurred on clients' computers. From this testing result, it is easy to tell us, in order to obtain a good performance, the number of the connected clients should be restricted to less than 60.

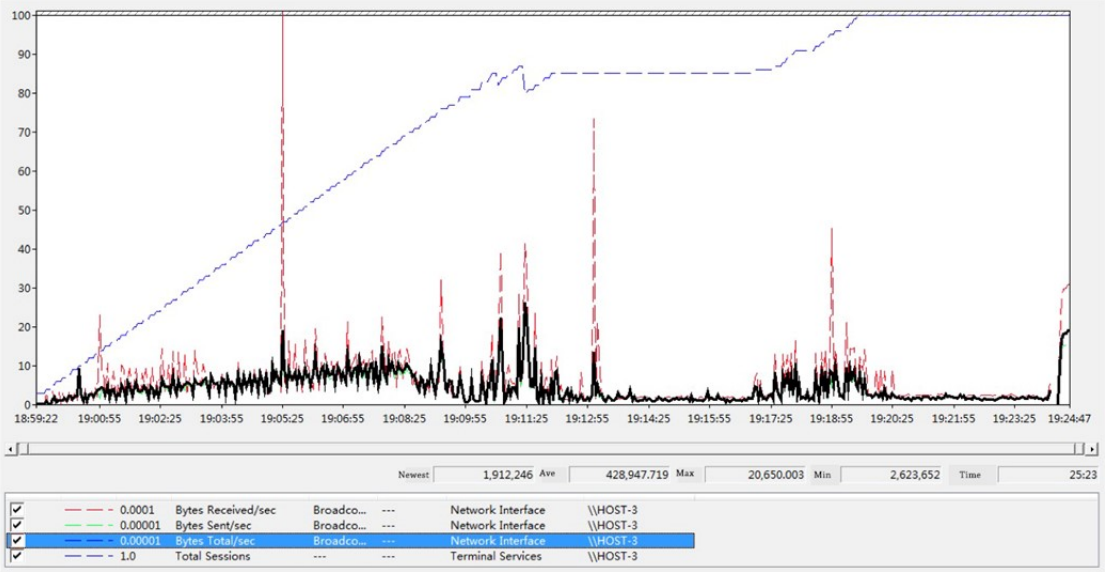

Figure 4.5 Network traffic

In Figure 4.4, the blue imaginary line is the total number of the clients being connected to this VDI system; the red imaginary line is the total number of the Bytes received in each second; the black solid line is the total number of the Bytes sent in each second. There is no large fluctuation, which means the network traffic is relatively stable.

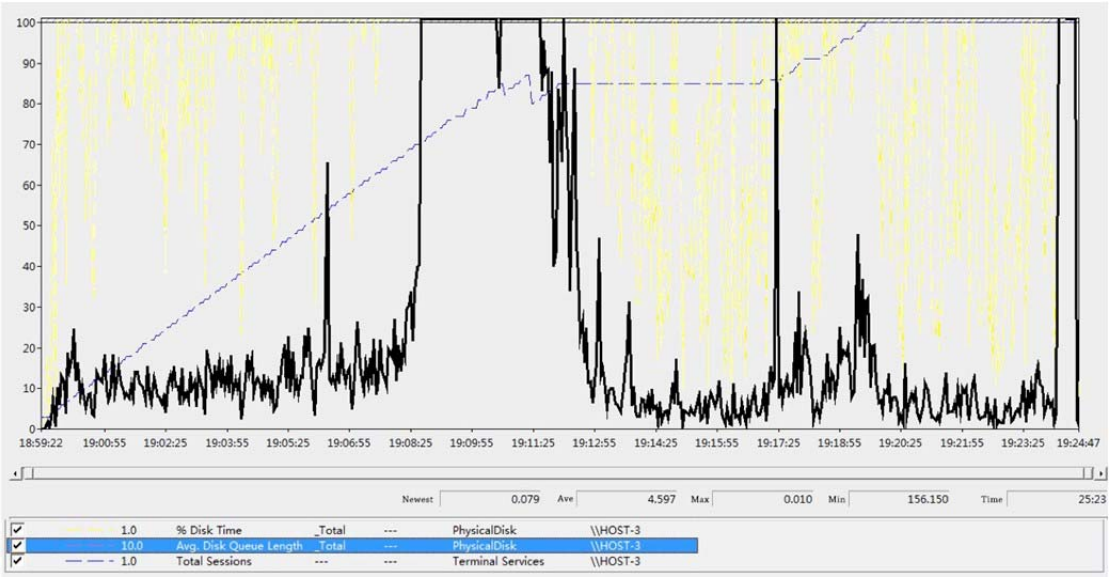

Figure 4.6 Disk performance

In the Figure 4.5, the blue imaginary line is the total number of the clients being connected to this VDI system; the black solid line is the average disk queue length; the yellow solid line is the delay time of the disk I/O transfer. Similar to Figure 4.3, once the number of the clients reaches 60, the disk I/O load increased abruptly.

From this testing we can see that, each server supports the maximum around 120 virtual machines simultaneously. But, if we expect to achieve the best performance, the number of the virtual machines should be around 60 and not over 70. From the Figure 3.6, there are totally five servers in the L-College's topology diagram. So, for this VDI thesis, the total number for the maximum virtual machines and the optimal virtual machines number are 750 and 350, respectively. If this VDI system is able to run 350 virtual machines at the same time with no delay, it has achieved the expected goals of this project.

4.3 Capacity Comparison Testing

The testing tools used in this testing is **Login VSI** (Login Virtual Session Indexer), a industry standard benchmarking tool is used to measure the performance and scalability in the testing phase of this VDI thesis by simulating one or more users' behavior, Login VSI allows a researcher to measure the maximum capacity of a VDI system expediently from three aspects (Berryman, Calyam & Honigford, 2010).

- Benchmarking: Compare the performance of different software tools and configurations in the L-College's environment.
- Load testing: Measure the performance and response times of specific infrastructure using the same applications, which have observed from the application management as discussed above.
- Change impact analysis: Predict the impact of any change in software on the performance of the testing VDI infrastructure by testing with realistic simulated workloads (Bose, Mishra, Sethuraman & Taheri, 2009).

In this experiment, we tested the capacity of three VDI system combinations, which includes VMware View + vSphere, Cirtrix XenDesktop + XenServer and XenDesktop + vSphere. For each combination, two different models of stress testing, heavy office only model and office with video model have been tested. According to Login VSI's introduction, when the VDI system starts being tested in a heavy office only model, the Login VSI will automatically run 7 specific operations several times, then record the average response times of each operation and weighted them. These 7 specific operations includes,

- Copy a document from the document pool in the home drive.
- Run Microsoft office Word application from the VDI server with a Word document (Weighted to 50%).
- Open a new Word document from the local client machine.
- Run Notepad application from the VDI server.
- Run the print dialogue within that Notepad application.
- Run the "Search and Replace" dialogue (Weighted to 500%).
- Run 7-zip from the VDI server to compress a file (Agrawal, Biswas & Nath, 2014).

For the office with video model, we used Windows Media Player to play a 1920× 1080P/60Hz video based on the heavy office only model.

The testing results from that 7 operations will be used to create a VSImax, which is used to calculate the total response times of those seven specific operations, called VSImax Classic Response Time (Reza & Byrd, 2013).

4.3.1 Testing methods

In this testing, we used the same network topology and hardware methods as we used in the Chapter 4.2 Functional Testing of VMware vSphere for the purpose of saving our labor. The software methods we used in this testing include,

- Citrix XenDesktop 5.6 FP1
- Citrix PVS 6.5
- Login VSI V4.0
- MS SQL Server 2008R2SP2
- VMware View
- VMware vSphere

The virtual desktop environment includes,

- Windows 7 32bit
- Microsoft office 2010
- Windows Media Player

4.3.2 View + vSphere Capacity Testing

- Heavy office only model

Table 4.5 Capacity testing result reports for vSphere+View 1

Test name	**Capacity_VMware_Office**
Test Description	VMware View + vSphere
VSImax v4	83 Sessions & Baseline 1412 ms
Benchmark mode	Disabled

VSI Threshold reached	Yes
VSIbaseline average response time (ms)	1412
VSImax average response time threshold (ms)	4756
VSImax threshold was reached at sessions	83
VSI response time threshold headroom	642
Sessions not responding	0
Corrected VSImax is	83
Total Sessions configured	100
Total Sessions successfully launched	100
Total Timeframe of test in seconds	3000
Average session launch interval in seconds	30.00
Amount of active launchers during test	2
Average session capacity per launcher	45

In the Table 4.5, it shows the capacity testing report when we use VMware View for desktop virtualization and VMware vSphere for server virtualization in a heavy office only testing environment. In this testing, all of 100 configured sessions have been launched. But the maximum number of the active sessions (VSImax threshold was reached at sessions) is only 83, because the office testing environment is fairly lightweight, so this figure does not look strong enough. The average response time is 1412 ms, which is acceptable.

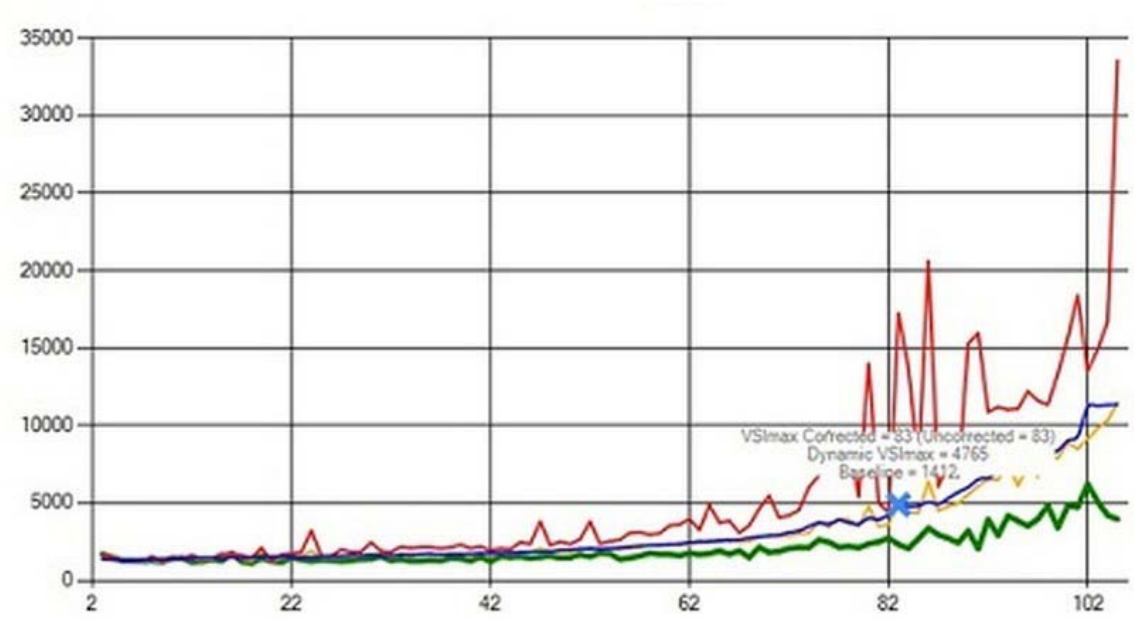

Figure 4.7 Active sessions analysis for vSphere+View 1

- Office + Video model

Table 4.6 Capacity testing results reports for vSphere+View 2

Test name	**Capacity_VMware_OfficeVideo**
Test Description	VMware View + vSphere
VSImax v4	56 Sessions & Baseline 1858 ms
Benchmark mode	Disabled
VSI Threshold reached	Yes
VSIbaseline average response time (ms)	1858
VSImax average response time threshold (ms)	4459
VSImax threshold was reached at sessions	56
VSI response time threshold headroom	338
Sessions not responding	0
Corrected VSImax is	56
Total Sessions configured	100
Total Sessions successfully launched	70
Total Timeframe of test in seconds	2100

Average session launch interval in seconds	30.00
Amount of active launchers during test	2
Average session capacity per launcher	35

In Table 4.6 and Figure 4.8, it shows the capacity testing reports when we use VMware View for desktop virtualization and VMware vSphere for server virtualization in an office and video testing environment. In this testing, only 70 out of 100 configured sessions have been launched. And the maximum number of the active sessions is only 56, which is much less than the figure in the office module. The average response time is 1858 ms, which grew around one-third.

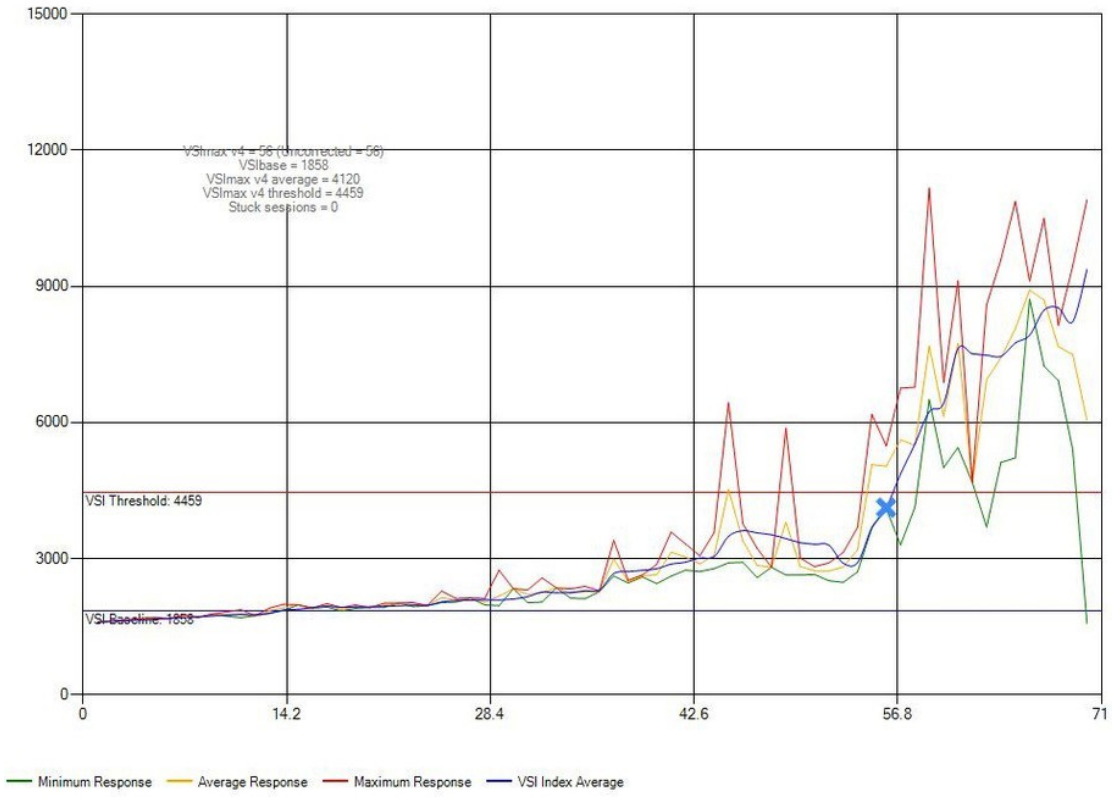

Figure 4.8 Active sessions analysis for vSphere+View 2

4.3.3 XenDesktop + XenServer Capacity Testing

- Heavy office only model

Table 4.7 Capacity testing results reports for XenDesktop+XenServer 1

Test name	**Capacity_Citrix_Office**
Test Description	Citrix XenDesktop + XenServer
VSImax v4	99 Sessions & Baseline 1738 ms
Benchmark mode	Disabled
VSI Threshold reached	Yes
VSIbaseline average response time (ms)	1738
VSImax average response time threshold (ms)	4339
VSImax threshold was reached at sessions	99
VSI response time threshold headroom	642
Sessions not responding	0
Corrected VSImax is	99
Total Sessions configured	100
Total Sessions successfully launched	100
Total Timeframe of test in seconds	3000
Average session launch interval in seconds	30.00
Amount of active launchers during test	2
Average session capacity per launcher	50

In the Table 4.7 and Figure 4.9, it shows the capacity testing result reports when we use Citrix XenDesktop for desktop virtualization and XenServer for server virtualization in a heavy office only testing environment. In this test, all of 100 configured sessions have been launched. And the maximum number of the active sessions is 99; this figure

reflects truth comparing to VMware View and vSphere. The average response time is 1738 ms, which is slightly slower than that of VMware View and vSphere, this may be because of the increase number in the aspect of the active sessions.

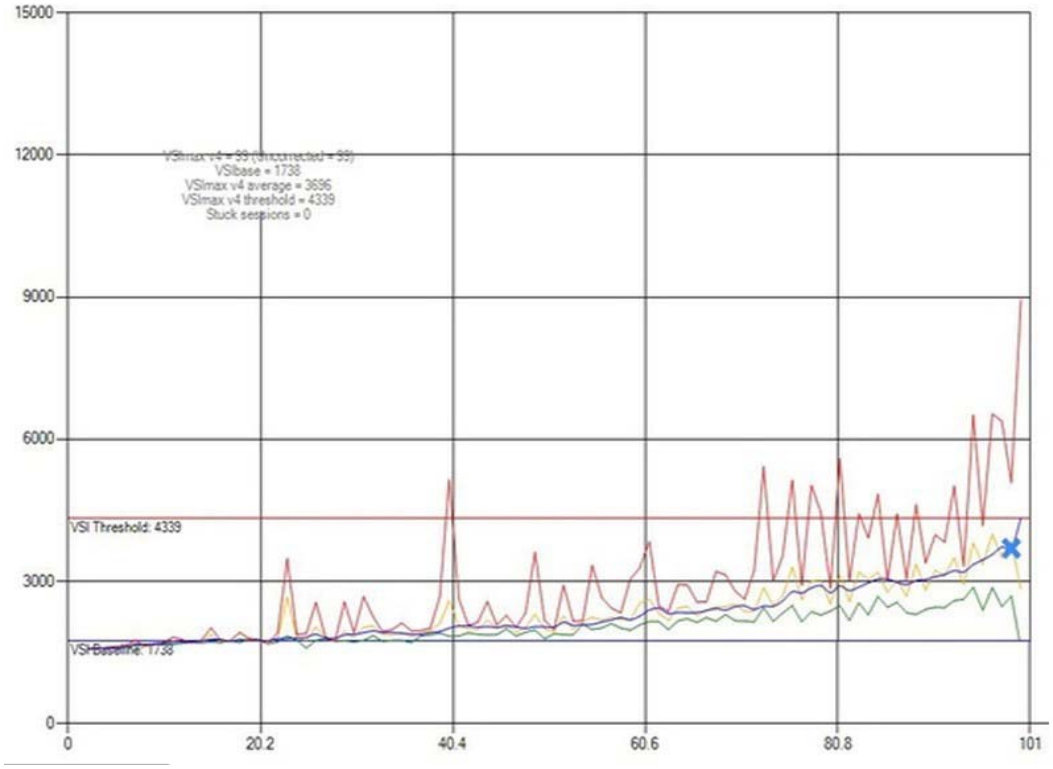

Figure 4.9 Active sessions analysis for XenDesktop+XenServer 1

- Office + Video model

Table 4.8 Capacity testing results reports for XenDesktop+XenServer 2

Test name	**Capacity_Citrix_OfficeVideo**
Test Description	Citrix XenDesktop + XenServer
VSImax v4	56 Sessions & Baseline 1858 ms
Benchmark mode	Disabled
VSI Threshold reached	Yes
VSIbaseline average response time (ms)	1858
VSImax average response time threshold (ms)	4459
VSImax threshold was reached at sessions	56

VSI response time threshold headroom	338
Sessions not responding	0
Corrected VSImax is	56
Total Sessions configured	100
Total Sessions successfully launched	70
Total Timeframe of test in seconds	2100
Average session launch interval in seconds	30.00
Amount of active launchers during test	2
Average session capacity per launcher	35

In Table 4.8, it shows the capacity testing result reports when we use Citrix XenDesktop for desktop virtualization and XenServer for server virtualization in an office with video testing environment. In this test, all of the figures are as same as the testing results when we use VMware View for desktop virtualization and VMware vSphere for server virtualization.

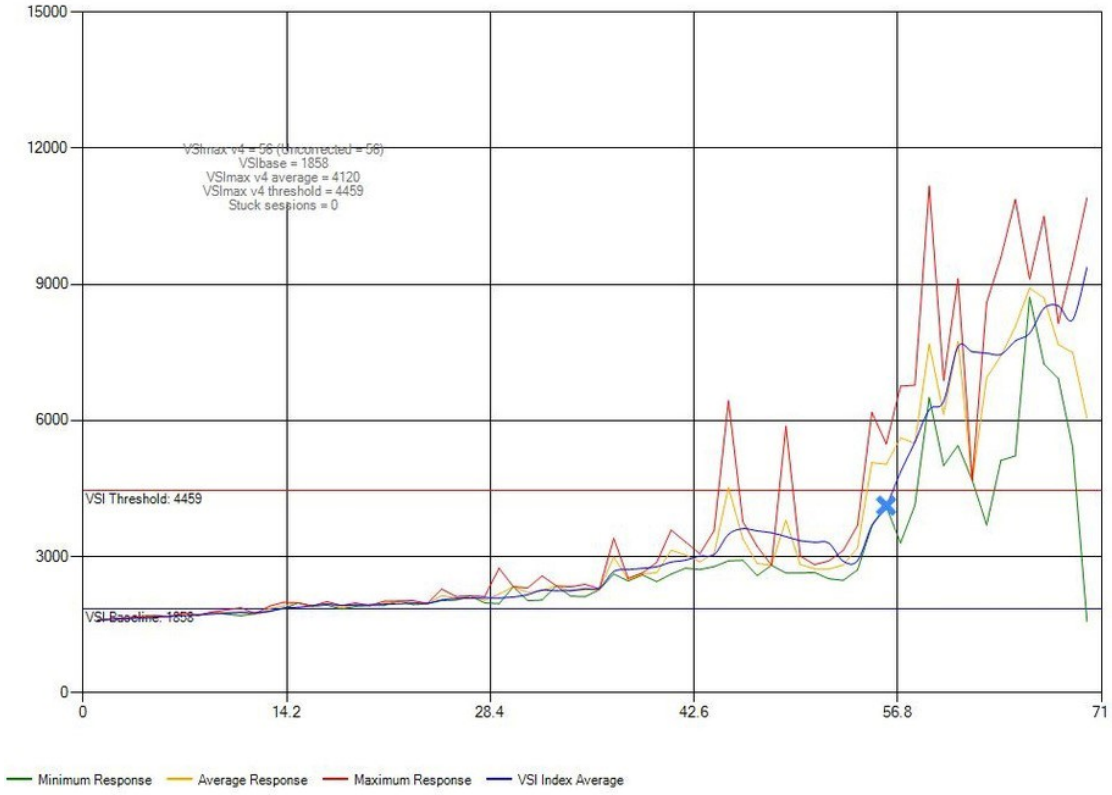

Figure 4.10 Active sessions analysis for XenDesktop+XenServer 2

4.3.4 XenDesktop + vSphere Capacity Testing

- Heavy office only model

Table 4.9 Capacity testing results reports for XenDesktop+vSphere1

Test name	**Capacity_Mix _Office**
Test Description	XenDesktop + vSphere
VSImax v4	99 Sessions & Baseline 1806 ms
Benchmark mode	Disabled
VSI Threshold reached	Yes
VSIbaseline average response time (ms)	1806
VSImax average response time threshold (ms)	4406
VSImax threshold was reached at sessions	99
VSI response time threshold headroom	638
Sessions not responding	1
Corrected VSImax is	99
Total Sessions configured	100
Total Sessions successfully launched	100
Total Timeframe of test in seconds	3000
Average session launch interval in seconds	30.00
Amount of active launchers during test	2

Average session capacity per launcher	50

In Table 4.9, it shows the capacity testing reports when we use Citrix XenDesktop for desktop virtualization and VMware vSphere for server virtualization in a heavy office only testing environment. In this test, all of 100 configured sessions have been launched. And the maximum number of the active sessions is 99, which is equal to the XenDesktop + XenServer, but better than View + vSphere. The average response time is 1858 ms, which is the worst one. Moreover, one session in this testing is not responded.

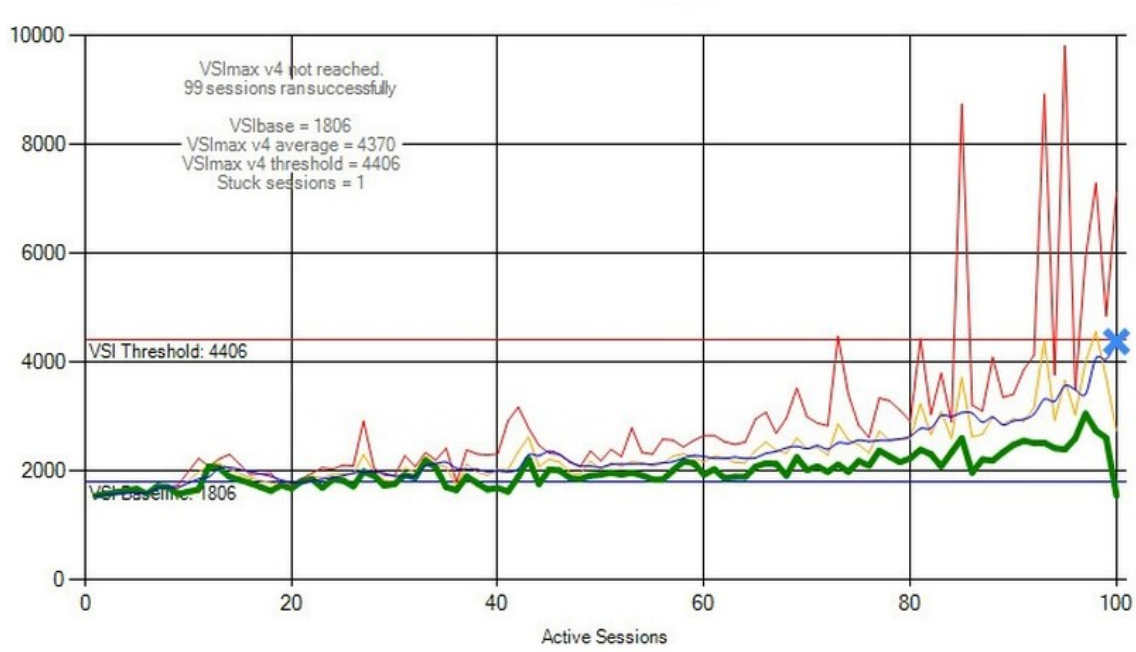

Figure 4.11 Active sessions analysis for XenDesktop+vSphere1

- Office + Video model

Table 4.10 Capacity testing results reports for XenDesktop+vSphere2

Test name	**Capacity_Mix _Office Video**
Test Description	XenDesktop + vSphere
VSImax v4	58 Sessions & Baseline 1732 ms
Benchmark mode	Disabled
VSI Threshold reached	Yes

VSIbaseline average response time (ms)	1732
VSImax average response time threshold (ms)	4333
VSImax threshold was reached at sessions	58
VSI response time threshold headroom	422
Sessions not responding	0
Corrected VSImax is	58
Total Sessions configured	100
Total Sessions successfully launched	70
Total Timeframe of test in seconds	2100
Average session launch interval in seconds	30.00
Amount of active launchers during test	2
Average session capacity per launcher	40

In Table 4.9, it shows the capacity testing reports when we use Citrix XenDesktop for desktop virtualization and VMware vSphere for server virtualization in an office with video testing environment. In this testing, 70 out of 100 configured sessions has been launched, the maximum number of the active sessions is 58. The average response time is 1732 ms.

4.3.5 Data Analysis

Table 4.11 Capacity Comparison

	View + vSphere		**XenDesktop+ XenServer**		**XenDesktop+ vSphere**	
Testing Module	Office	Office Video	Office	Office Video	Office	Office Video
VSImax threshold was reached at sessions	83	56	99	56	99	58

VSIbaseline average response time (ms)	1412	1858	1738	1858	1806	1732
Sessions not responding	0	0	0	0	1	0

Table 4.11 listed three key figures in the six testing scenarios. After compared with them, we see that in the heavy office with only testing environment, both of XenDesktop + Xeon Server combination and VMware View + vSphere combination has better capabilities than those of XenDesktop + vSphere combination, in all aspects of the maximum number of the active sessions, the average response time and the number of sessions not responding. In the office with video testing environment, XenDesktop + Xen Server combination and VMware View + vSphere combination has a same result, but XenDesktop + vSphere combination has a small edge in both aspects of the maximum number of the active sessions and the average response time. This shows that the XenDesktop + vSphere combination is able to work well in high-stress environments, such as in handling images, videos or animations in a VDI system.

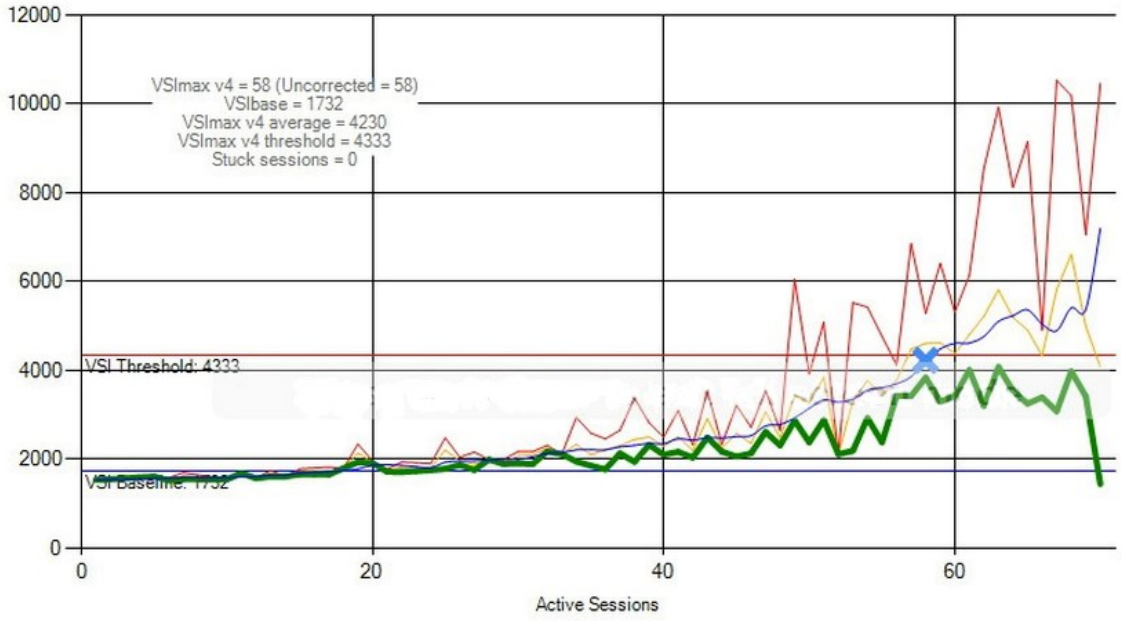

Figure 4.12 Active sessions analysis for XenDesktop+vSphere2

Chapter 5 Conclusion and Future Work

The VDI system is able to tremendously decrease hardware costs, greatly increase end users' experience in productivity and mobility, and provide vast flexibility for applications and operating systems. But apparently designing a well performance and high secure VDI system is very challengeable.

Based on reviewing the previous VDI researches and studies of other products associated with virtualization technology, in this thesis we raise the research problems of how to design and development a stability secure VDI system. In the thesis, we describe a secure VDI system for the campus environment of the L-College, which has integrated different VDI tools from various IT vendors, such as Citrix XenDesktop, View Composer, VMware View Manager and VMware vSphere.

In order to make sure the stability of this VDI system in the convention processing from physical to virtual, we study the virtualization technology of P2V conversion and its reliability. Three categories of work have been conducted including the research work of disk space capacity allocation and the integration service during the P2V conversion process, the application test of reliability upon the virtualization operation and the research work on the high availability of virtual machines on the cluster node of virtual architecture.

In the aspect of security, the architecture has been verified, and we have also introduced VLAN into the VDI system to defend those potential attacks.

The results from all of the functional testing, performance testing and capacity testing show that the proposed VDI system is able to match the entire requirement. Specifically the XenDesktop + vSphere combination is able to work well in high-volume environments. It means that this VDI system is suitable for most of the high volume application, which consumes large amounts of CPU or memory resources. There is one expectation for further work is, from Chapter 3.4, in order to calculate the number of the kernel of the CPU, the memory and the network I/O, which could be provided to the virtual applications from the physical server, we have modified the

ideal calculation formulas advised from Citrix. So there may have some errors with the testing of VMware and Microsoft products. It could be useful to modify the resource allocation advised by VMware and Microsoft as well, and introduced the updated formulas to the test.

References

Agrawal, S., Biswas, R., & Nath, A. (2014). Virtual Desktop Infrastructure in Higher Education Institution: Energy Efficiency as an Application of Green Computing. In *IEEE Fourth International Conference on Communication Systems and Network Technologies.* Bhopal India (pp. 601-605).

Agarwal, S., & Nath, A. (2014). Desktop Virtualization and Green Computing Solutions. In *Proceedings of the Second International Conference on Soft Computing for Problem Solving*. Springer, India (pp. 1439-1449).

Almeida, J., Almeida, V., Ardagna, D., Cunha, I. Francalanci, C. & Trubian, M. (2010). Joint Admission Control and Resource Allocation in Virtualized Servers. *Journal of Parallel and Distributed Computing*, *70*(4), 344-362.

Alvarez, C. (2011). NetApp Deduplication for FAS and V-Series Deployment and Implementation Guide. *Technical Report, 35*(5), 231.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & Zaharia, M.

(2010). A View of Cloud Computing. *Communications of the ACM*, *53*(4), 50-58.

Arwidmark, J., & Nystrm, M. (2011). Deploying Physical and Virtual Servers Using MDT 2010 and SCVMM 2008 R2. *Deployment Fundamentals, 34* (2), 23-76.

Asai, H. (2013, September). P2V Migration with Post-Copy Hot Cloning for Service Downtime Reduction. In *Proceedings of the International Conference on Cloud and*

Green Computing (pp. 1-8). IEEE.

Baek, S. J., Park, S. M., Yang, S. H., Song, E. H., & Jeong, Y. S. (2010). Efficient Server Virtualization using Grid Service Infrastructure. *Journal of Information Processing Systems*, *6*(4), 553-562.

Baratto, R. A., Potter, S., Su, G., & Nieh, J. (2004). Mobidesk: Mobile Virtual Desktop Computing. In *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking,* Philadelphia USA (pp. 1-15).

Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., & Warfield, A. (2003). Xen and the Art of Virtualization. *ACM Special Interest Group on Operating Systems (SIGOPS) Operating Systems Review*, *37*(5), 164-177.

Basak, D., Toshniwal, R., Maskalik, S., & Sequeira, A. (2010). Virtualizing Networking and Security in the Cloud. *ACM Special Interest Group on Operating Systems (SIGOPS) Operating Systems Review*, *44*(4), 86-94.

Bazargan, F. A., Yeun, C. Y., & Zemerly, J. (2011). Understanding the Security Challenges of Virtualized Environments. In *IEEE International Conference on Internet Technology and Secured Transactions (ICITST)*, Abu Dhabi UAE (pp. 67-72).

Beaty, K., Kochut, A., & Shaikh, H. (2009). Desktop to Cloud Transformation Planning. In *IEEE International Parallel & Distributed Processing Symposium*, Roma Italy (pp. 1-8).

Beloglazov, A., Abawajy, J., & Buyya, R. (2012). Energy-aware Resource Allocation Heuristics for Efficient Management of Data Centers for Cloud Computing. *Future Generation Computer Systems*, *28*(5), 755-768.

Beloglazov, A., & Buyya, R. (2010). Energy Efficient Resource Management in

Virtualized Cloud data Centers. In *Proceedings of the 10th IEEE/ ACM International Conference on Cluster, Cloud and Grid Computing,* Melbourne Australia (pp. 826-831).

Berryman, A., Calyam, P., Honigford, M., & Lai, A. M. (2010). Vdbench: A Benchmarking Toolkit for Thin-client Based Virtual Desktop Environments. In *IEEE Second International Conference on Cloud Computing Technology and Science.* Indiana USA (pp. 480-487).

Bobroff, N., Kochut, A., & Beaty, K. (2007). Dynamic Placement of Virtual Machines for Managing Sla Violations. In *Integrated Network Management 10th IFIP/IEEE International Symposium,* Munich Germany (pp. 119-128).

Bolte, M., Sievers, M., Birkenheuer, G., Niehorster, O., & Brinkmann, A. (2010). Non-intrusive Virtualization Management Using Libvirt. In *Design, Automation & Test in Europe Conference & Exhibition (DATE),* Dresden Germany (pp. 574-579).

Bose, S., Mishra, P., Sethuraman, P., & Taheri, R. (2009). Benchmarking Database Performance in a Virtual Environment. In *Performance Evaluation and Benchmarking*, Heidelberg Germany (pp. 167-182).

Calder, B., Chien, A. A., Wang, J., & Yang, D. (2005). The Entropia Virtual Machine for Desktop Grids. In *Proceedings of the 1st ACM/USENIX International Conference on Virtual Execution Environments,* Utah USA (pp. 186-196).

Carbone, J., & Larson, R. (2009). *Windows Server 2008 Hyper-V Resource Kit*. Pearson Education.

Cerling, T., & Buller, J. L. (2011). *Mastering Microsoft Virtualization*. John Wiley & Sons.

Chaudhary, V., Cha, M., Walters, J. P., Guercio, S., & Gallo, S. (2008). A Comparison of Virtualization Technologies for HPC. In *22nd International Conference on Advanced Information Networking and Applications.* Okinawa, Japan (pp. 861-868).

Das, T., Padala, P., Padmanabhan, V. N., Ramjee, R., & Shin, K. G. (2010). LiteGreen: Saving Energy in Networked Desktops using Virtualization. In *USENIX Annual Technical Conference*, Boston USA (pp. 26-34).

Dasilva, D. A., Liu, L., Bessis, N., & Zhan, Y. (2012). Enabling Green IT through Building a Virtual Desktop Infrastructure. In *IEEE Eighth International Conference on Semantics, Knowledge and Grids (SKG)*, Beijing China (pp. 32-38).

Deuby, S. (2009). SCVMM 2008's Virtual Machine Templates-System Center Virtual Machine Manager's VM Template Feature Lets You Quickly and Consistently Provision VMs. *Windows IT Pro*, *2009*(175), 20.

Dittner, R., & Rule Jr, D. (2011). *The Best Damn Server Virtualization Book Period: Including Vmware, Xen, and Microsoft Virtual Server*. Syngress.

Feng, X., Tang, J., Luo, X., & Jin, Y. (2011). A Performance Study of Live VM Migration Technologies: VMotion vs XenMotion. In *SPIE/OSA/IEEE Asia Communications and Photonics*, Shanghai China (pp. 83101B-83101B).

Golden, B. (2008). *Virtualization for Dummies*, NJ: Wiley Publishing, Inc.

Greamo, C., & Ghosh, A. (2011). Sandboxing and Virtualization: Modern Tools for Combating Malware. *Security & Privacy, IEEE*, *9*(2), 79-82.

Grossman, R. L. (2009). The Case for Cloud Computing. *IT professional*, *11*(2), 23-27.

Guo, Z. (2012). Build of a Lightweight Desktop Virtualization Environment Based on VMware View. *Science Mosaic*, *4*(23), 11.

Hannifin, D. (2010). *Microsoft Windows Server 2008 R2 Administrator's Reference: The Administrator's Essential Reference*. Syngress.

Haletky, E. (2007). *VMware ESX Server in the Enterprise: Planning and Securing Virtualization Servers*. Pearson Education.

Haletky, E. (2009). *VMware vSphere and Virtual Infrastructure Security: Securing the Virtual Environment*. Pearson Education.

Herrod, S. (2006). The Future of Virtualization Technology. *Computer Architecture News*, *34*(2), 352.

Hodgman, M. R. (2013). Desktop Virtualization: Applications And Considerations. *Contemporary Issues in Education Research (CIER)*, *6*(1), 123-132.

Hoffmann, P., Schumann, R., Maksoud, T. M. A., & Premier, G. C. (2010). Virtual Commissioning of Manufacturing Systems–A Review and New Approaches for Simplification. In *Proceedings 24th European Conference on Modelling and Simulation*, Kuala Lumpur Malaysia (pp. 175-181).

Huber, N., Quast, M., Hauck, M. & Kounev, S. (2011). Evaluating and Modeling Virtualization Performance Overhead for Cloud Environments. In *1st International Conference on Cloud Computing and Service Science,* Noordwijkerhout, Netherlands (pp. 563-573).

Hung, C. P., & Min, P. S. (2010). Infrastructure Arrangement For Application Virtualization Services. In *The 9th International Information and*

Telecommunication Technologies Symposium, Rio de Janeiro Brazil (pp. 78-85).

Hwang, J., Suh, S. B., Heo, S. K., Park, C. J., Ryu, J. M., Park, S. Y., & Kim, C. R. (2008). Xen on ARM: System Virtualization Using Xen Hypervisor for ARM-based Secure Mobile Phones. In *IEEE Consumer Communications and Networking Conference.* Las Vegas USA (pp. 257-261).

Hwang, J., & Wood, T. (2012). Adaptive Dynamic Priority Scheduling for Virtual Desktop Infrastructures. In *Proceedings of the IEEE 20th International Workshop on Quality of Service*, Coimbra Portugal (pp. 16-17).

James, G. R. (2010). *Citrix XenDesktop Implementation: a Practical Guide for IT Professionals*. Elsevier.

Janssen, R. (2010). VDI and Security. *Network Security*, 3, 8-11.

Jang, S. M., Choi, W. H., & Kim, W. Y. (2013). Client Rendering Method for Desktop Virtualization Services. *ETRI Journal*, *35*(2), 348-351.

Jin, L., & Miyazawa, T. (2002). MRM Server: a Context-aware and Location-based Mobile E-commerce Server. In *Proceedings of the 2nd International Workshop on Mobile Commerce*, Atlanta USA (pp. 33-39).

Kadupatil, A., Patil, S., Shaha, S., Sarode, S., & Nair, S. (2013). SCVMM Driver for Libvirt. *International Journal*, *1*(7), 7-17.

Kalyvianaki, E., Charalambous, T., & Hand, S. (2009). Self-adaptive and Self-configured

CPU Resource Provisioning for Virtualized Servers Using Kalman Filters. In *Proceedings of the 6th International Conference on Autonomic Computing*, New

York USA (pp. 117-126).

Khanna, G., Beaty, K., Kar, G., & Kochut, A. (2006). Application Performance Management in Virtualized Server Environments. In *10th IEEE/IFIP Network Operations and Management Symposium,* Vancouver Canada (pp. 373-381).

Kouril, J., & Lambertova, P. (2010). Performance Analysis and Comparison of Virtualization Protocols, RDP and PCoIP. In *Proc. of Intemational Conference on Computers.* Greece (pp. 782-787).

Li, J., Jia, Y., Liu, L., & Wo, T. (2013). Cyber Live App: A Secure Sharing and Migration Approach for Live Virtual Desktop Applications in a Cloud Environment. *Future Generation Computer Systems*, *29*(1), 330-340.

Li, Y., Sun, J., Zheng, Z., & Shen, H. (2012). Research of University Disaster Recovery System Based on Virtualization Technology. In *Information Computing and Applications*, Heidelberg, Germany (pp. 110-116).

Liao, X., Jin, H., Hu, L., & Liu, H. (2010). Towards Virtualized Desktop Environment. *Concurrency and Computation: Practice and Experience*, *22*(4), 419-440.

Liu, J., & Lai, W. (2010). Security analysis of VLAN-based Virtual Desktop Infrastructure. In *International Conference on Educational and Network Technology*, Jiangsu China (pp. 301-304).

Lo, J. (2005). *VMware and CPU Virtualization Technology*. World Wide Web Electronic Publication.

Lowe, S. (2011). *Mastering VMware vSphere 5*. John Wiley & Sons.

Lowe, S., & Marshall, N. (2013). *Mastering VMware vSphere 5.5*. John Wiley & Sons.

Man, C. L. T., & Kayashima, M. (2011). Virtual Machine Placement Algorithm for Virtualized Desktop Infrastructure. In *IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS),* Beijing China (pp. 333-337).

Martin, A. (2008). *The Ten Page Introduction to Trusted Computing*, Oxford University.

Mashtizadeh, A., Celebi, E., Garfinkel, T., & Cai, M. (2011). The Design and Evolution of Live Storage Migration in VMware ESX. In *Proceedings of the USENIX Annual Technical Conference*, Berkeley USA (pp. 14-14).

Mell, P., & Grance, T. (2009). The NIST Definition of Cloud Computing. *National Institute of Standards and Technology*, *53*(6), 50.

Michael, M., & Linares, H. (2011). *Mastering Virtual Machine Manager 2008 R2*. John Wiley & Sons.

Miller, K., & Pegah, M. (2007). Virtualization: Virtually at the Desktop. In *Proceedings of the 35th Annual ACM SIGUCCS fall Conference.* Florida USA (pp. 255-260).

Mousa, M. A. (2012). Virtualization Technology| Revolution of Virtual Desktop Infrastructure. *Journal of Technical Science and Technologies*, *1*(1), 17-23.

Murphy, A. (2001). *Enabling Long Distance Live Migration with F5 and VMware vMotion*. F5 Networks, Inc.

Nelson, M., Lim, B. H., & Hutchins, G. (2005). Fast Transparent Migration for Virtual Machines. In *USENIX Annual Technical Conference,* Berkeley USA (pp. 391-394).

Nishikiori, M. (2011). Server Virtualization with VMware vSphere 4. *Fujitsu Scientific and Technical Journal*, *47*(3), 356-361.

O'doherty, P. (2012). *VMware View 5: Building a Successful Virtual Desktop*. VMware Press.

Padala, P., Shin, K. G., Zhu, X., Uysal, M., Wang, Z., Singhal, S. & Salem, K. (2007). Adaptive Control of Virtualized Resources in Utility Computing Environments. *ACM SIGOPS Operating Systems Review*, *41*(3), 289-302.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3).

Principato, M. (2010). Virtualization Technology and Process Control System Upgrades. In *52nd IEEE-IAS/PCA Cement Industry Technical Conference,* Colorado USA (pp. 1-12).

Ranadive, A., & Davda, B. (2012). Toward a Paravirtual vRDMA Device for VMware ESXI Guests. *VMware Technical Journal, Winter 2012*, *1*(2).

Ranganathan, K., & Foster, I. (2002). Decoupling Computation and Data Scheduling in Distributed Data-intensive Applications. In *IEEE Conference on High Performance Distributed Computing International Symposium*, Edinburgh, Scotland (pp. 352-358).

Reza, S., & Byrd, T. (2013). Reducing Migration-induced Misses in an Over-subscribed

Multiprocessor System. *Parallel Processing Letters*, *23*(01).

Rhee, J., Kochut, A., & Beaty, K. (2009). DeskBench: Flexible Virtual Desktop Benchmarking Toolkit. In *IFIP/IEEE International Symposium on Integrated Network Management,* New York USA (pp. 622-629).

Ruest, N., & Ruest, D. (2009). *Virtualization, A Beginner's Guide*. McGraw-Hill, Inc..

Sahoo, J., Mohapatra, S., & Lath, R. (2010). Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues. In *IEEE 2010 Second International Conference on Computer and Network Technology (ICCNT)*, Bangkok Thailand (pp. 222-226).

Sailer, R., Jaeger, T., Valdez, E., Caceres, R., Perez, R., Berger, S., & Doorn, L. (2005, December). Building a MAC-based Security Architecture for the Xen Open-source Hypervisor. In *IEEE 21st Annual Computer Security Applications Conference,* Tucson, USA (pp. 10-pp).

Sands, R., Hsieh, G., Hendricks, W., & Williams, A. (2012). Building a Secure Virtual Lab Infrastructure for IT Education, *Review of Higher Education & Self-Learning*, *4*(13).

Scarfone, K. (2011). *Guide to Security for Full Virtualization Technologies*. DIANE Publishing.

Shamma, M., Meyer, D. T., Wires, J., Ivanova, M., Hutchinson, N. C., & Warfield, A. (2011). Capo: Recapitulating Storage for Virtual Desktops. In *9th USENIX Conference on File and Storage Technologies*, California USA (pp. 31-45).

Sharma, U., Shenoy, P., Sahu, S., & Shaikh, A. (2011). A Cost-aware Elasticity Provisioning System for the Cloud. In *31st International Conference on Distributed Computing Systems (ICDCS),* Minneapolis, USA (pp. 559-570).

Sindoori, R., Pallavi, V. P., & Abinaya, P. (2013). An Overview of Disaster Recovery in Virtualization Technology. *Journal of Artificial Intelligence*, *6(13)*, 60-67.

Sotomayor, B., Montero, R. S., Llorente, I. M., & Foster, I. (2009). Virtual Infrastructure Management in Private and Hybrid Clouds. *IEEE Internet Computing, 13*(5), 14-22.

Sun, Y., & Chen, Y. X. (2012). Research on Desktop Virtualization and its Security. *Information Security and Communications Privacy*, *6(24)*, 2-41.

Urgaonkar, R., Kozat, U. C., Igarashi, K., & Neely, M. J. (2010). Dynamic Resource Allocation and Power Management in Virtualized Data Centers. In *IEEE Network Operations and Management Symposium (NOMS),* Osaka Japan(pp. 479-486).

Velte, A., & Velte, T. (2009). *Microsoft Virtualization with Hyper-V*. McGraw-Hill, Inc.

Ventresco, J. (2013). *Implementing VMware Horizon View 5.2*. Packt Publishing Ltd.

Villanueva, B., & Cook, B. (2005). Providing Students 24/7 Virtual Access and Hands-on

Training using Mware GSX Server. In *Proceedings of the 33rd Annual ACM Special Interest Group on University and College Computing Services (SIGUCCS),* New York, USA (pp. 421-425).

Waldspurger, C. A. (2002). Memory Resource Management in VMware ESX Server. *ACM SIGOPS European Workshop*, Saint-Emilion, France (pp. 181-194).

Williams, D. E. (2007). *Virtualization with Xen: Including XenEnterprise, XenServer, and XenExpress,* Syngress.

Wöhrmann, B., Schäfer, C., Baumgart, G., Kügow, O., Alder, U. S., & Brunner, M. (2012). *VMware vSphere 5*. Galileo Press.

Yan, L. (2011). Development and Application of Desktop Virtualization Technology. In *IEEE 3rd International Conference on Communication Software and Networks (ICCSN),* Xian China (pp. 326-329).

Younge, A. J., Henschel, R., Brown, J. T., Von Laszewski, G., Qiu, J., & Fox, G. C. (2011). Analysis of Virtualization Technologies for High Performance Computing Environments. In *IEEE International Conference on Cloud Computing (CLOUD).* Washington, USA (pp. 9-16).

Nong, F. & Fang, L., (2012). Deduplication Based Storage Optimization Technique for Virtual Desktop. *Journal of Computer Research and Development*, 1(43), 7-15.

Yan, L. (2011). Development and Application of Desktop Virtualization Technology. In *IEEE 3rd International Conference on Communication Software and Networks,* Beijing, China (pp. 326-329).

Yu, H. E., Pan, Y. L., Wu, C. H., Chen, H. S., Chen, C. M., & Cheng, K. Y. (2013). On-Demand Automated Fast Deployment and Coordinated Cloud Services. In *IEEE 5th International Conference on Cloud Computing Technology,* Honolulu, Hawail, USA (pp. 252-255).

Yu, H., Xiao, X., Zhao, Y., & Zheng, W. (2013). BIRDS: a Bare-metal Recovery System for Instant Restoration of Data Services. *IEEE Transactions on*

Computers, *1(54)*, 26.

Yu, P., Cao, J., Wen, W., & Lu, J. (2006). Mobile Agent Enabled Application Mobility for Pervasive Computing. In *Ubiquitous Intelligence and Computing,* Heidelberg, Germany (pp. 648-657).

Zhang, L. J., & Zhou, Q. (2009). CCOA: Cloud Computing Open Architecture. In *IEEE International Conference on Web Services,* Los Angeles, USA (pp. 607-616).

Zhang, Y., Juels, A., Reiter, M. K., & Ristenpart, T. (2012). Cross-VM Side Channels and Their Use to Extract Private Keys. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security,* Raleigh, USA (pp. 305-316).