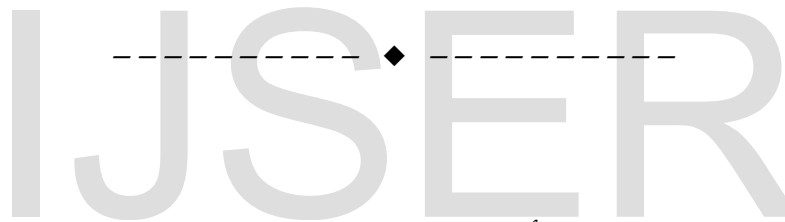# A Proposed Approach for Deploying Network Attached Storage by Configuring   Virtual Switch In ESXi

Maria Andleeb Siddiqui, Hammad Kamal

Abstract— The main focus in this paper is the Deployment of Network Attached Storage (NAS) in virtualized environment as it has been the subject for many researchers because of the significance presence of Network-Attached Storage in the datacenter. The consideration for the choice tends to hinge on the issue of cost, performance, availability and ease of manageability. Therefore VMware vSphere is the considerable solution which explains how to configure the ESXi system so that it can use and manage different types of storage. For simplification of the ESXi host configuration, Active Directory is used for user authentication as it also reduces the risk for configuration issues that could lead to the unauthorized access. For many virtualization deployments, running vSphere on NAS is a viable option because when configured correctly, it offers strong performance and stability. Therefore this paper provides an overview to deploy NAS (Network Attached Storage) by using vSphere. For this purpose DNS (Domain Name Space) and AD (Active Directory) is implemented in vSphere client. NFS (Network file System) and SAN (Storage area Network) will be implemented in another virtual machine so that only those files can be accessed by the machine in ESXi whose Domain name is present in Active Directory. NFS storage was introduced as a storage resource that can be shared across a cluster of VMware vSphere ESXi hosts. To make the networking feasible an ESXi switch is configured first.

Index Terms— Active Directory, Domain, ESXi, NAS (Network Attached Storage), vSphere, NFS (Network file System), SAN

————————————————— ◆ —————————————————

1 INTRODUCTION:

Many researchers are leading toward deployment of virtualized environments with Network Attached Storage (NAS) that shared storage resources because of the significant presence of Network File system Storage (NFS) in the datacenter today, as well as the lower cost-per-port for IP based Storage.

The use of Network Attached Storage (NAS) has become increasingly popular when it comes to virtualized Environment. IT professionals at small and mid market organizations cited ease of deployment and

1. Have a virtual switch configured for IP based storage.

———————————————

- *Maria Andleeb Siddiqui is currently enrolled in PhD program in Computer Science in N.E.D University of Engineering and Technology, Pakistan,*
  E-mail: maria_13augi@hotmail.com

- *HammadKamal is currently pursuing masters degree program in Business Administration in Institute of Business Administration, Pakistan,*
  E-mail: hammadkhan001@hotmail.com

ease of management as two of the features over capabilities that would drive their organizations to deploy a NAS environment [1]. Using NFS to support virtual server environment provides advantages for IT managers in terms of cost and complexity. Cost is the most important benefit of using NFS to support a virtual server platform. Having shared storage is almost a must with virtualization to take advantage of some of the more advanced features, such as high availability, that require shared storage. Before NFS storage can be addressed by an ESXi server, the following issues need to be addressed:

2. The ESXi hosts needs to be configured to enable its NFS client as shown in Figure 1.

3. The NFS storage server needs to have been configured to export a mount point that is accessible to the ESXi server on a trusted network.

Figure 1: Model of deployment of NAS using vSphere ESXi

vSphere Client is an interface used to connect remotely to VMware vCenter Server from a Windows system.It is an interface used to remotely connect to an ESXi host or a vCenter Server from a Windows PC as shown in Figure 3. vSphere Client can be downloaded in two ways :

- Use the VMware Infrastructure Management Installer.

- Download the client from the vCenter Server system or an ESXi host.

VMware ESXi is an operating system-independent hypervisor based on the VM kernel operating system interfacing with agents that run atop it. ESXi is the exclusive hypervisor for VMware vSphere 5.x licenses as shown in Figure 2.
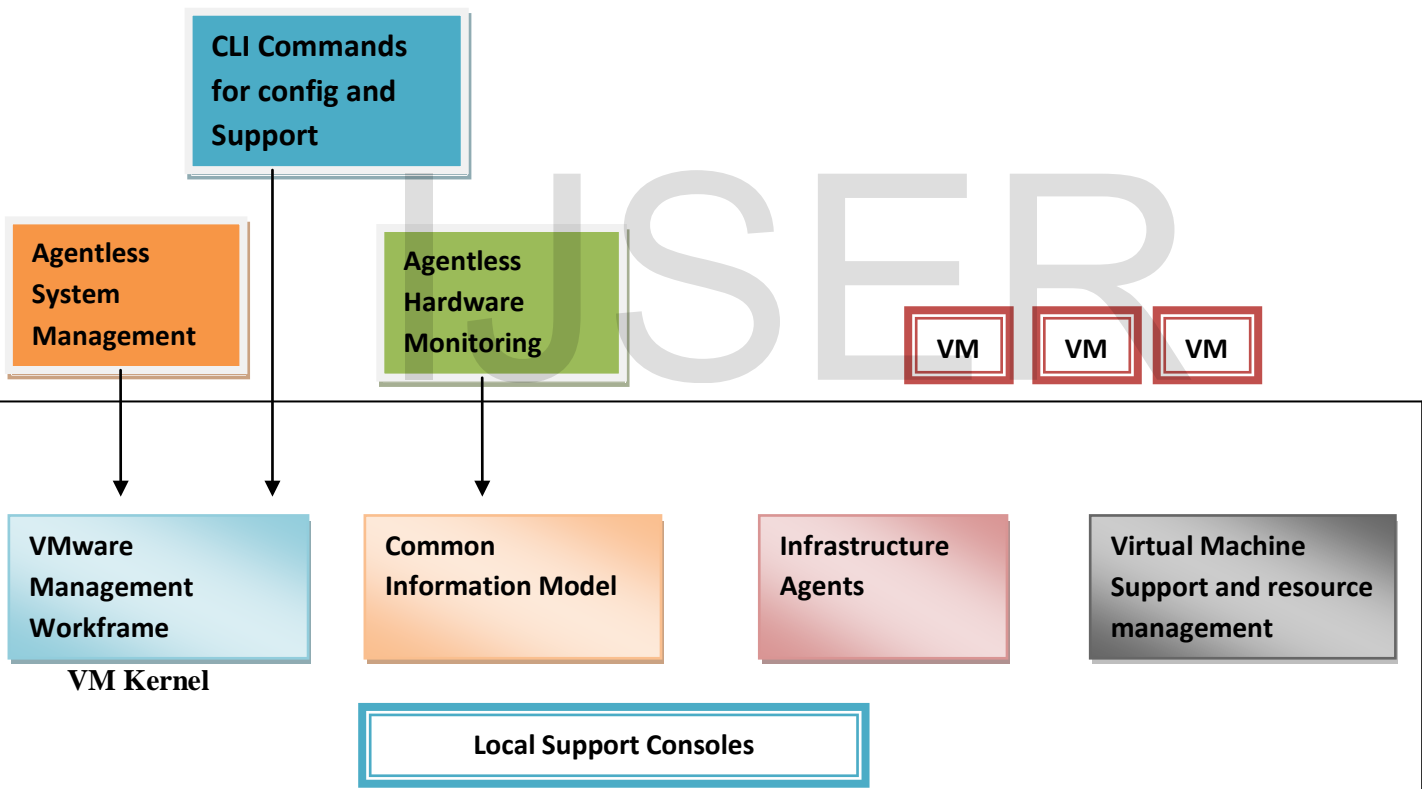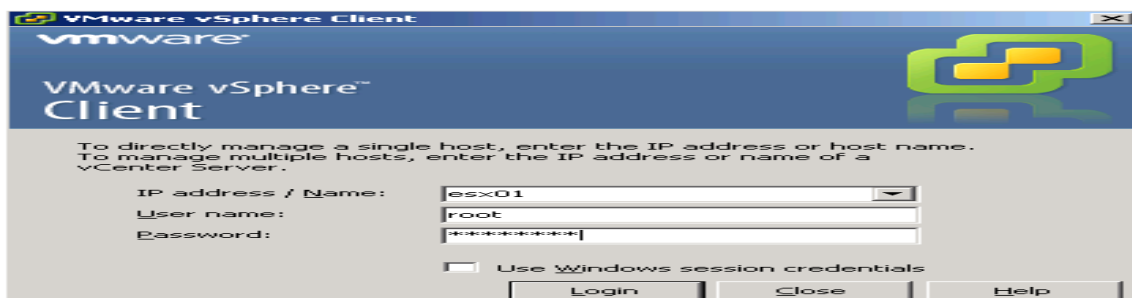

Figure 2: ESXi Architecture

Figure 3: vSphere Client management

Therefore the idea under consideration in this paper is to deploy NAS by configuring virtual switch in the ESXi host as NAS offers many clear advantages while not suffering the previous realized performance limitation. The deployment of NAS in virtualized environment consist of several phases which includes configuration of ESXi host, configuration of virtual switch, connection of ESXi host with vsphere client, installation of active

2 LITERATURE REVIEW

Virtualization technologies resulted in widespread usage by finding important applications over a wide range of areas such as server consolidation, secure computing platforms, supporting multiple operating systems, system migration, virtual local area network (VLAN) etc. Virtualization is considered to be the act of abstracting the physical boundaries of a technology. There are several ways of occurrence of physical abstraction, including optimizes security, flexibility, fault tolerance, power efficiency, and performance. Virtual machines are separate entities from one another. Therefore if one of them fails, they are completely isolated from all the other software on that physical machine, including other virtual machines. This greatly increases security, because problems can be contained [2]. Two types of hypervisors are defined for server virtualization the term hypervisor was coined for the

storage and the client on the network. This concept which was demonstrated indicates how network attached devices can eliminate the server as a bottleneck and thus improving both performance and scalability. The experimentation, graphical representation, and results are obtained to explain the advantage of secured network devices over the classical store and forward process [5]. A method to overcome limitation of existed methods for storage virtualization uses grouping of Metadata Center and Volume driver for managing virtual volume. The virtualization software or device is responsible for maintaining a consistent view of all the mapping information for the virtualized storage. This information is usually scaled meta-data and is stored as

directory (AD) to configure the DNS and routing information for an ESXi host and configuration of ESXi host as NTP client. The rest of the paper is organized as follows. The subsequent section present the related work based on review of previous work. Section III presented the proposed methodology with the configuration results. Conclusion and future work is presented in section   IV.

software operating above Kernel which was known as the supervisor in mainframes. One of the hypervisor is native or bare metal hypervisor runs directly on the host, computer's hardware and another is a hosted hypervisor, runs within an operating system environment (OSE) [3]. One of the methodologies proposed was Dataplexed NAS System (Dataplexed Network Attached Storage System), a cross-platform distributed file system, which provides strong security and client/server heterogeneity both at hardware and operating system level. This system aimed to resolve the problems associated with traditional client/server systems, namely the high performance requirements, and costly maintenance of the computing resources [4]. A Network Storage virtualization model (NSVM) is presented to demonstrate how the cloud can be utilized to transfer data directly between

a mapping table. This method consists of a Metadata Center that stores data about data at the common place. Volume Driver accesses the data path from the Meta data centre and presents virtual volumes path every server by sending instruction to server [6].A novel intrusion detection scheme is proposed to merge the two methods with multi-source information fusion technology. The fusion optimization strategy is provided to guarantee that the fusion scheme can make a more accuracy decision for the suspicious behaviors with more information gathered from different levels of the system. Also the intrusion detection modules in the new scheme can be self-learning and update the profiles by themselves. Experimental results demonstrate that the

over capability of new fusion intrusion detection scheme increased by 15% [7]. In distributed storage system, storage service provider (SSP) is a critical component to receive and response the requests from client. Therefore a real-time and flexible management of SSP is presented. With the advantages from virtualization and cloud computing, the states of SSP main VM are observed by another isolated virtual machine, and the administrator can inspect the storage service provider through the uniform management interface in real-time [8].

3   METHODOLOGY AND CONFIGURATION RESULTS:

The proposed methodology consists of the following phases:

3.1 Configuration of ESXi as NTP Client:

The first phase of deployment focused on configuring ESXi on virtual machines as shown in Figure 4(a). The Direct Console User interface (DCUI) is similar to the

BIOS of a computer with the keyboard-only interface. The DSUI allows an administrator to set a root password and enable or disable lock down mode. The network settings i.e.   Host name, IP configuration and DNS server can be modified. Then the ESXi host is configured as a NTP client as shown in Figure 4(b). NTP is a client server protocol used to synchronize a computer's clock to a time reference. In this phase finally the DNS and routing phase is configured on ESXi host to change the host name and search domains.

3.2 Installation of vCenter Server:

ESXi host communicate with the vCenter server. For this purpose we install the vcenter server. vCenter architecture consist of vSphere client, additional modules, database server and Active directory domain which all interact with the ESXi host as shown in Figure 5 (a). vCenter is installed with the set of default plug-ins. It is installed to import the ESXi server and configure the network and time zone setting as shown in Figure 5(b).
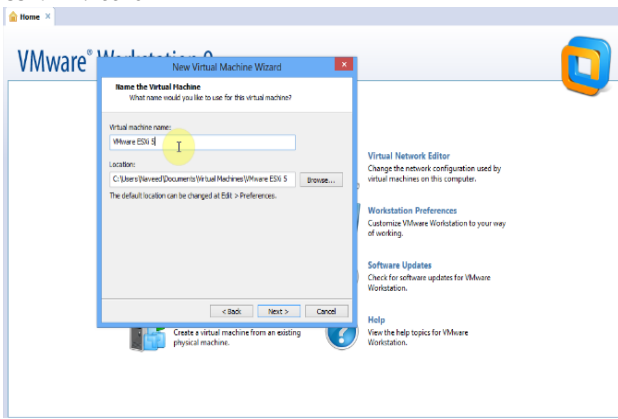
Figure 4(a): Installation of ESXi on Virtual Machine
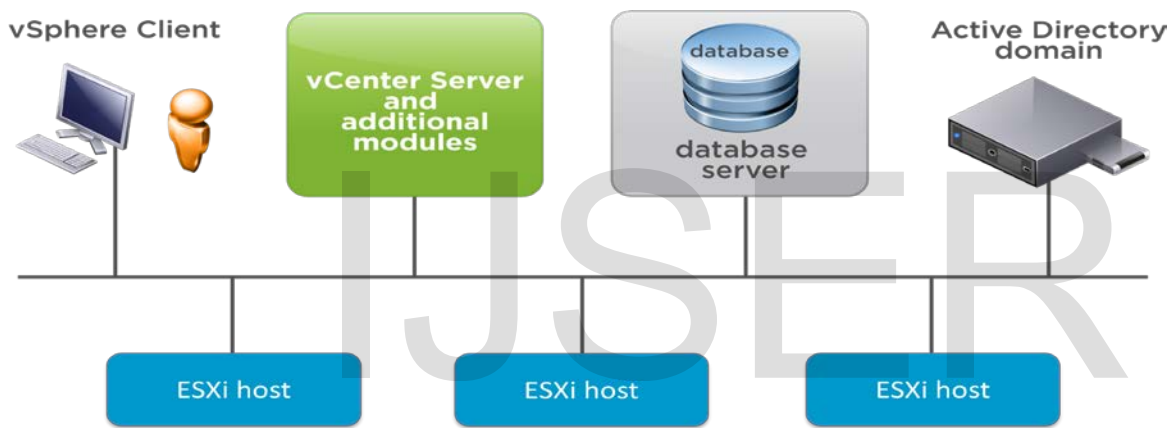

Figure 4(b): Loading state of ESXi module.

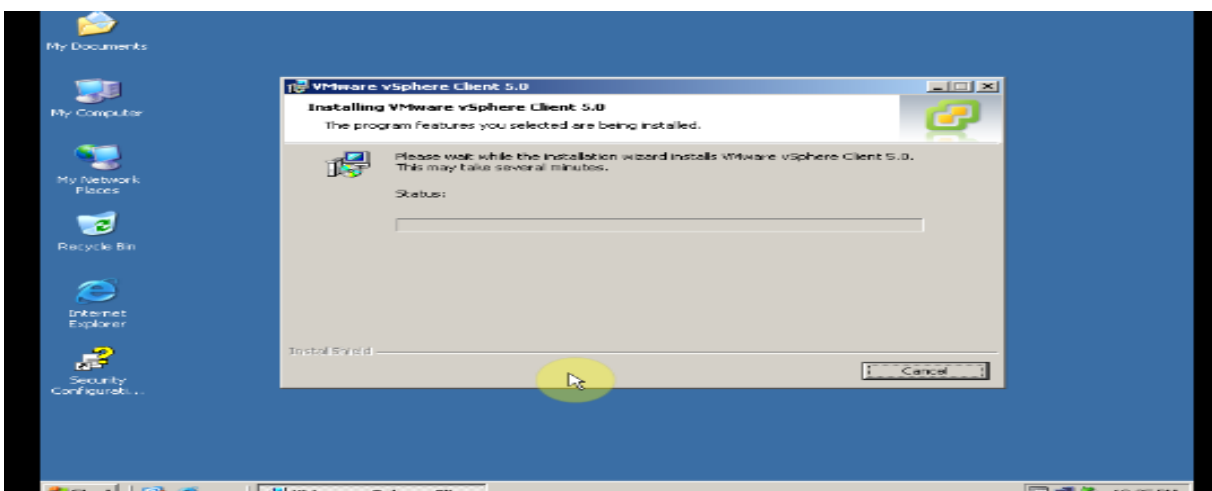**Figure 5(a): vCenter Architecture**.

Figure 5(b): Installation of VMware Vsphere Client 5.0

3.3 Configuration of the Virtual Switch:

This phase focused on virtual switch configuration. ESXi supports 802.1 QVLAN tagging as shown in Figure 6(a). Virtual tagging is one of the three tagging policies supported:

i) Packets from a virtual machine are tagged as they exit the virtual switch.

ii) Packets are untagged as they return to the virtual machine.

iii) Affect on performance is minimal.

There are three network policies on standard virtual switch port. They are security, traffic shaping and NIC teaming policies as shown in Figure 6(b).

Security policies are configured at the standard virtual switch and at the port groups. For controlling a virtual machines network bandwidth, network traffic shaping is used. NIC teaming settings include load balancing, network failure detection, notify switches failback.
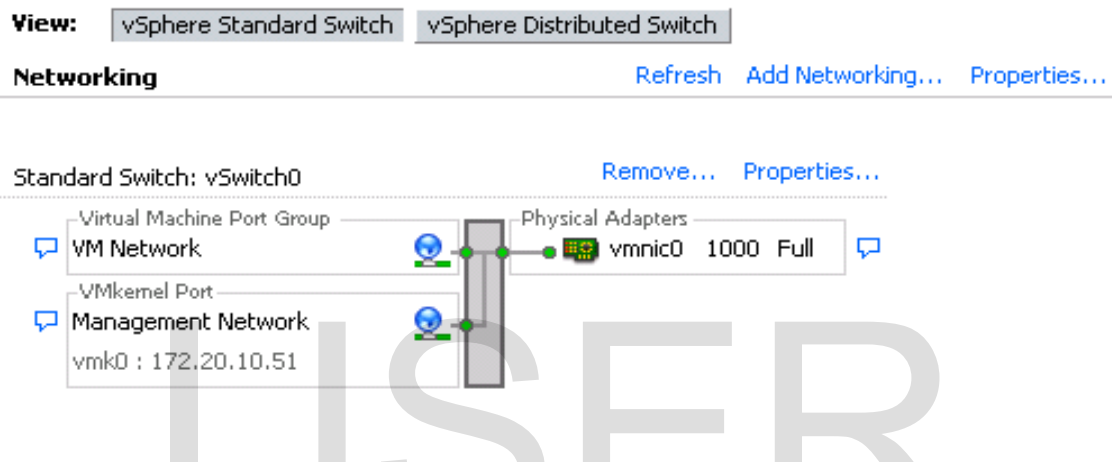

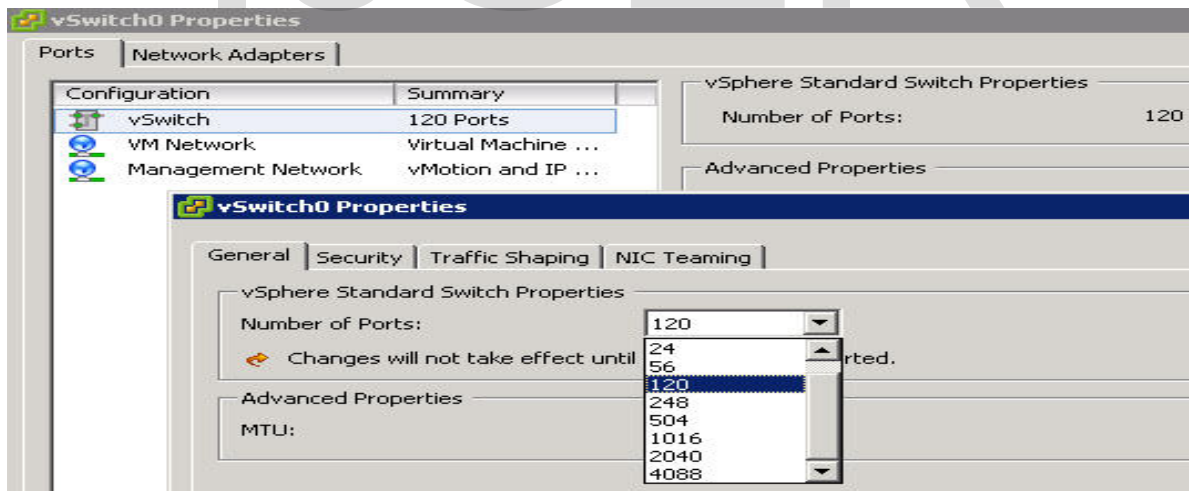**Figure 6(a): Configuration of ports of Virtual Switch**

Figure 6(b): The network policies of standard virtual switch ports

3.4 Installation of Active Directory:

In this phase, DNS (Domain Name Space) and AD (Active Directory) is implemented inVsphere client as shown

in Figure 7. ESXi can access only those files whose Domain name is present in Active Directory.
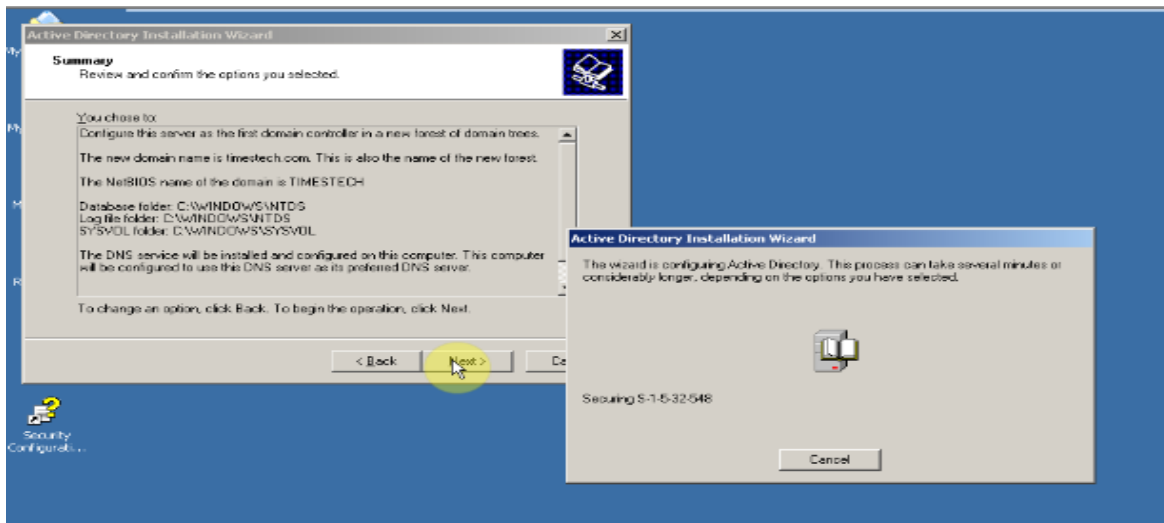

Figure 7: Installation of Active Directory and DNS setting

3.5 Configuration of NAS/NFS Storage

The final phase of deployment is to hold the virtual machines files, templates and ISO images, for which the data stores are used as shown in Figure 8(a). NFS is a storage shared over the network at the file system level. It supports NFS version 3 over TCP/IP. In order to deploy the network attached storage a VMKernel is created for the better storage performance as shown in Figure 8(b). Then the following information is provided:

i)   NFS server name (or IP address)
ii)   Folder on the NFS server
iii)   Whether to mount the NFS file system, read only as default is to mount read/write.
iv)   NFS datastore name as shown in Figure 8(c)

StarWind virtual SAN (VSAN) is leading software defined storage for Microsoft Windows Server 2012 R2 and Microsoft Hyper-V 3.0. StarWind software is used to create a fault-tolerant shared storage of the hypervisor resources as it follows the VMware VSA concept also, and operates inside a VM on the ESXi host as shown in Figure 8(d).

In order to deploy a true SAN over an IP network using standard Ethernet switches, StarWind allows any IT administrator to build high availability SAN at affordable price.
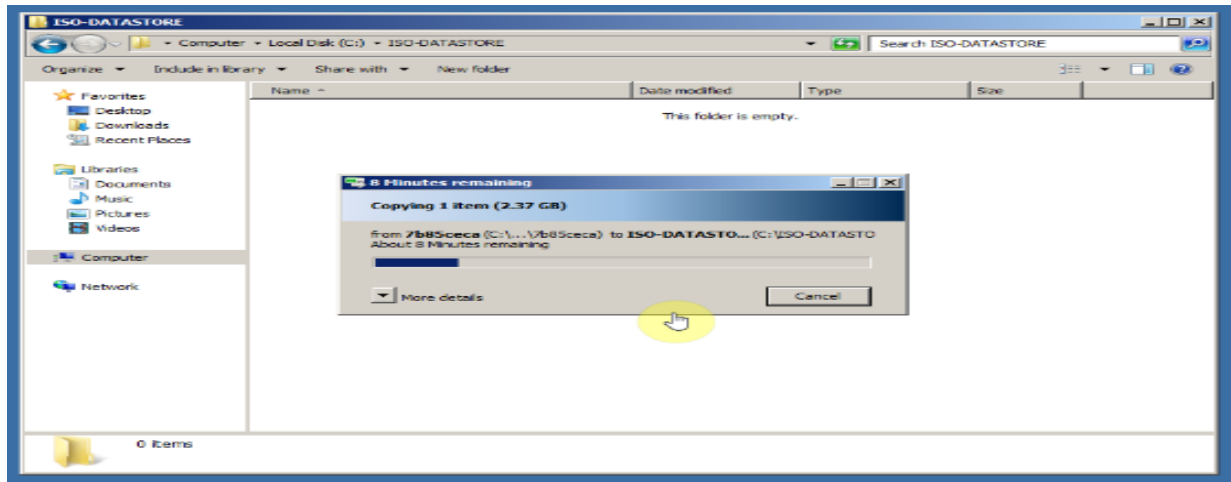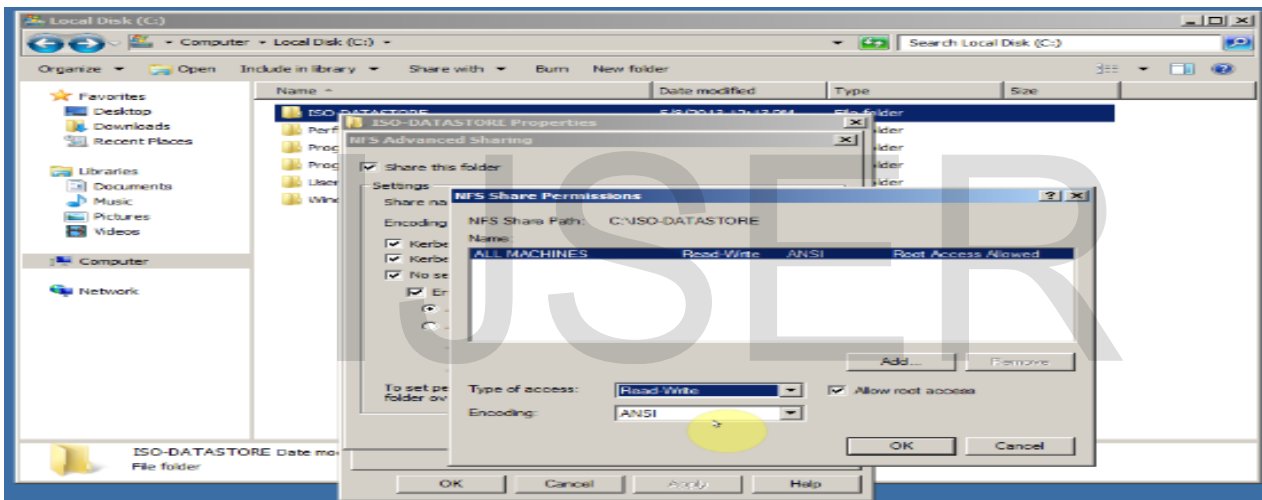
Figure 8(a): ISO Datastore
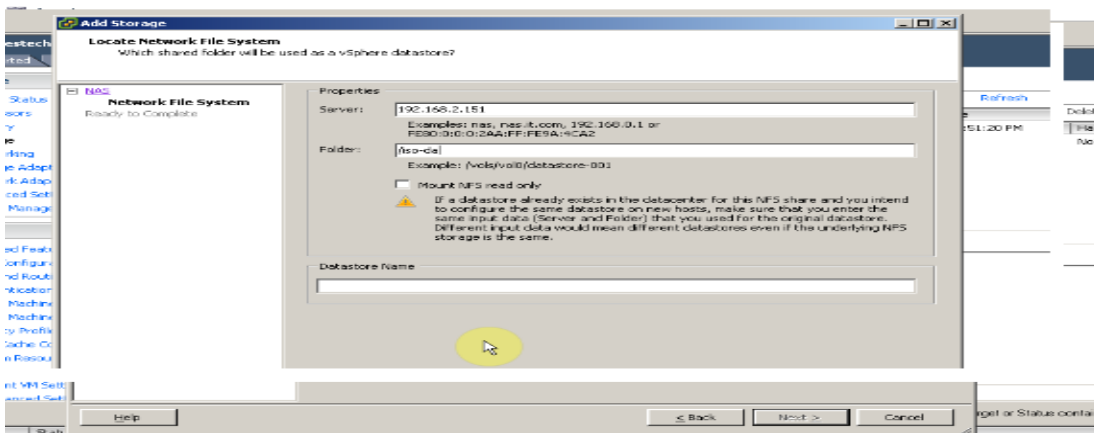

Figure 8(b): NFS Share permissions

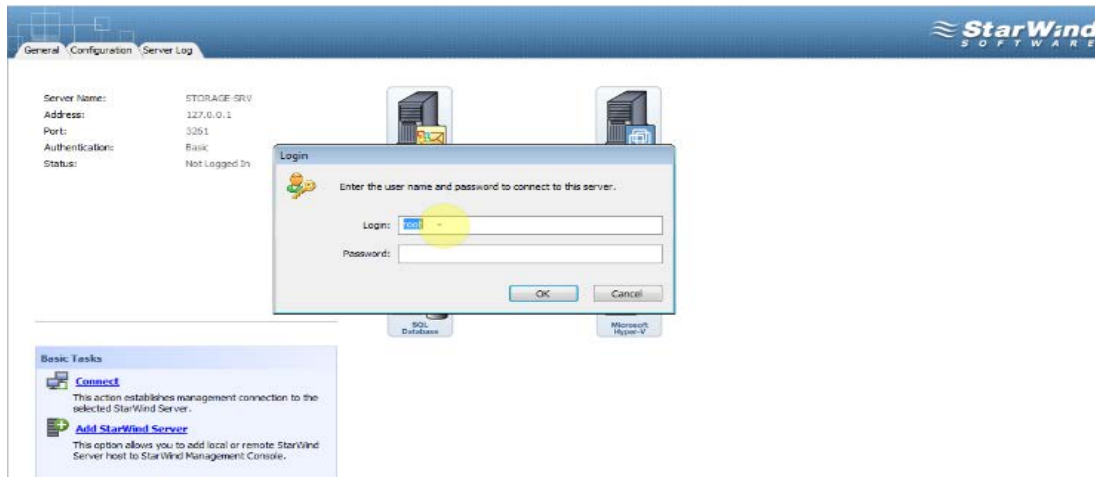**Figure 8(c): Configuration of ISO datastore and management of NFS**

Figure 8(d): Configuration of starwind software.

4 CONCLUSION AND FUTURE WORK

This paper proposed the deployment of network attached storage by incorporating the configuration of virtual switch technology. This proposed methodology will improve the performance and scalability of file server than when the server handles the processes of store and forwards.It also helps to store and access the files through one central location. There is a growing need to share documents easily and securely via the network among businesses worldwide. In future, security can be implemented in Network attached Storage by using an authentication model to secure the storage from hacker.

REFERENCES

[1]. Aviv Kaufmann and Michael Leon, "New VNX2: Real World benefits for virtualized NAS workloads", *ESG Lab review*, November, 2013.

[2]. Pankaj Dwivedi, "Application of Virtualization Technology in Networked Computing System", *International Journal of Electronics and Communication Engineering and Technology*, 3(1), 2014 ,165-174.

[3]. John Wiley & Sons, Inc and Hoboken, "Server Virtualization for Dummies", *Oracle Special edition*, 2012, fromhttp://www.oracle.com/oms/hardware/extremeperformance/assets/ept-eb-dummies-server-1641465.pdf

[4]. Praveen Vijai, Minnu Meria, Midhu Babu, "Dataplexed Network Attached Storage System", *International Journal of Science and research*, *Vol. 3,*February 2014, 119-121. [5]. Li-zhong Geng and Hui-bo jia, "A Novel Intrusion Detection Scheme for Network Attached Storage Based on Multi-source Information Fusion*", IEEE conf. on Computational Intelligence and Security,* Beijing, 2009, 469-473. [6]. Benard Ong'era Osero, "Network Storage Virtualization and Management", *International Journal of Education and Research,1(12),2013.* [7]. Mrs. Dhanamma Jagli, Mr. Ramesh Solanki, Mrs Rohini Temkar and Mrs. Laxmi Vershapogu, "Semi Symmetric Method of Storage Virtualization*" International Journal of Information Technology Convergence and Services, 2(6),* December 2012, 23-29.

[8]. Longbo Ran and Hai Jin," Real Time and Flexible Management of Storage Service Provider in Distributed Storage, *International Journal of Hybrid Information Technology, 5(2),* April 2012, 219-224