HELSINKI METROPOLIA UNIVERSITY OF APPLIED SCIENCES

Bachelor's Degree in Information Technology

Bachelor's Thesis

HYPER-V HIGH AVAILABILITY WITH LOW COST HARDWARE COMPONENTS

Author: Juha Petteri Honkanen
Instructor: Kari Järvi
Instructor: Panu Palmu

Approved: __. __. 2010

Kari Järvi, LicSc (Tech)
Principal Lecturer

Metropolia

PREFACE

The main focus of this study was to build a guide for a company called Datapalvelut.net. The guide was needed for educational purposes and to give information about the Microsoft clustering. From this study I learnt a lot about the clustering techniques and from different clustering platforms although they are not introduced in the present study.

The most important thing that I learnt was that the clustering is an easy and rather cheap way to gain benefits to organizations that need to rely their business heavily on the server software and information.

I would like to thank the Datapalvelut.net and my instructor Panu Palmu for his guidance and advice. I am also thankful to my language inspector Jonita Martelius who helped me with the language correction of the study. Finally my loving family earns the biggest thanks for their support and the motivation they gave me.

Tuusula, October 24, 2010

Juha Honkanen

Metropolia

ABSTRACT

Name: Juha Honkanen

Title: HYPER-V HIGH AVAILABILITY WITH LOW COST HARDWARE COMPONENTS

Date: October 24, 2010 **Number of pages:** 43

Degree Programme:
Telecommunication

Instructor: Kari Järvi, Principal Lecturer

Instructor: Panu Palmu, Chief Executive Officer

Many organizations store their crucial information and business tools to the servers that are not always available. When the server is unavailable the organization could lose huge amounts of money or the business could totally end if the crucial information were lost.

This study is to give instructions for building a high available Hyper-V virtualized environment. The objective of the study was to test and analyse the possibility to build a high available server environment with low cost server hardware. The low cost server hardware was used because many small organizations do not use high available environments because they do not have the budget to build high-end high available information technology environment.

The study was made for a company called Datapalvelut.net and it serves as a guide on how to build a basic two node failover cluster providing high available virtual machine services.

Key words: Failover Clustering, Hyper-V, Windows Server 2008 R2, High availability

Metropolia

OPINNÄYTETYÖN TIIVISTELMÄ

Työn tekijä: Juha Honkanen	
Työn nimi: HYPER-V HIGH AVAILABILITY WITH LOW COST HARDWARE COMPONENTS	
Päivämäärä: 24.10.2010	**Sivumäärä:** 43 s.
Koulutusohjelma: Tietoliikennetekniikka	**Ammatillinen suuntautuminen:** ITCom
Työn ohjaaja: Kari Järvi, Yliopettaja **Työn ohjaaja:** Panu Palmu, Toimitusjohtaja	

Monet organisaatiot tallentavat elintärkeitä tietoja ja työvälineitä palvelimille, jotka eivät ole aina käytettävissä. Kun palvelin ei ole käytettävissä, organisaatio voi menettää valtavia rahamääriä tai liiketoiminta voi loppua, jos tärkeää tieto häviää.

Tämän työn tarkoituksena on toimia ohjeena Hyper-V -virtualisoitujen ympäristöjen korkean saatavuuden luomisessa. Työn tavoitteena oli tutkia ja analysoida mahdollisuutta rakentaa korkean saatavuuden palvelinympäristö halvalla palvelinraudalla. Halpaa palvelinrautaa käytettiin, koska monet pienet organisaatiot eivät käytä korkean käytettävyyden ympäristöä, koska niillä ei ole budjettia rakentaa korkealaatuista korkean käytettävyyden tietotekniikkaympäristöä.

Työ on tehty Datapalvelut.net -yritykselle ja sen tarkoituksena on toimia ohjeena, miten rakennetaan kahden palvelimen vikasietoinen klusteri, joka tarjoaa korkean saatavuuden virtuaalikoneita.

Avainsanat: Failover Clustering, Hyper-V, Windows Server 2008 R2, High availability

TABLE OF CONTENTS

PREFACE

ABSTRACT

TIIVISTELMÄ

TABLE OF CONTENTS

(LIST OF ILLUSTRATIONS/ GRAPHS/ FIGURES/ TABLES)

ABBREVIATIONS/ACRONYMS

1 INTRODUCTION 1

2 CLUSTERING SYSTEMS 3

2.1 Clustering History 3

2.2 Clustering Basics 3

2.3 Evolution of Microsoft Clustering Service 5

2.4 Failover Clustering on Windows Server 2008 and Windows Server 2008 R2 11

3 TESTING ENVIRONMENT AND METHOD 13

3.1 Hardware Equipment 13

3.1.1 Server 13

3.1.2 Network 15

3.1.3 Storage 16

3.2 Building Failover Cluster Environment 16

3.2.1 Pre-installation of Software 16

3.2.2 Network Configurations 18

3.2.3 Storage Configurations 21

3.2.4 Failover Cluster Feature Configurations 24

3.2.5 Configure Hyper-V Virtual Machine with High Availability 29

4 TESTING FAILOVER CLUSTER 36

4.1 Controlled Failures of Failover Cluster 36

4.2 Unexpected Failures of Failover Cluster 37

5 RESULTS AND ANALYSIS 38

5.1 Controlled Failures of Failover Cluster 38

5.2 Unexpected Failures of Failover Cluster 39

6 DISCUSSION AND CONCLUSIONS 41

REFERENCES 44

LIST OF ILLUSTRATIONS/ GRAPHS/ FIGURES/ TABLES

Tables

Table 1 Maximum number of nodes in one cluster of different Windows Operating System versions [5] 6
Table 2 Available resources in NT 4.0 cluster [6, Chapter 1] 8
Table 3 Results of the Controlled Failures 39
Table 4 Results of the Unexpected Failures 40

Figures

Figure 1 Node Majority Quorum Model 9
Figure 2 Node and Disk Majority Quorum Model 10
Figure 3 Node and File Share Majority Quorum Model 10
Figure 4 No Majority: Disk Only Quorum Model 11
Figure 5 Hewlett Packard Proliant ML 320 G6 Server [9] 14
Figure 6 Hewlett Packard Proliant ML 110 G4 Server [10] 14
Figure 7 Zyxel NGB-417N Wireless Router 15
Figure 8 Zyxel ES-108A Ethernet Switch 15
Figure 9 QNAP TS-239 PRO II Storage System 16
Figure 10 QNAP Finder Software 17
Figure 11 Physical Network Card Configuration As Virtual Network Card 19
Figure 12 Hyper-V Virtual Network Manager Configurations 19
Figure 13 Graphical View of the Environment 20
Figure 14 QNAP Storage Systems iSCSI Configurations 21
Figure 15 iSCSI Target Configurations 22
Figure 16 Disk Management View Before Disk Partitioning 23
Figure 17 iSCSI LUNs Taken Online On Node Server 23
Figure 18 Multipath Configurations with Fail Over Only Policy 24
Figure 19 Server Roles and Features 25
Figure 20 Cluster Validation Tool Servers Listed 26
Figure 21 Validation Tool Tests Selection Page 27
Figure 22 Validatition Tool Validating Tests 27
Figure 23 Cluster Name Configuration 28
Figure 24 Installing New Hyper-V Virtual Machine 29
Figure 25 Hyper-V Virtual Machine Configuration Page 1 30
Figure 26 Hyper-V Virtual Machine Configuration Page 2 31
Figure 27 Hyper-V Virtual Machine Configuration Page 3 31
Figure 28 Hyper-V Virtual Machine Configuration Page 4 32
Figure 29 Hyper-V Virtual Machine Configuration Page 5 33
Figure 30 Installing Operating System on Clustered Virtual Machine 33
Figure 31 Virtual Machine Processor Configurations 34
Figure 32 Second Virtual Machine Location and Name Configuration 35
Figure 33 Second Virtual Machine Hard Disk Configurations 35

ABBREVIATIONS/ACRONYMS

LAN	Local Area Network
WAN	Wide Area Network
NASA	North American Satellite Authority
MSCS	Microsoft Cluster Server
iSCSI	SCSI Protocol Over TCP/IP (IETF draft standard)
SCSI	Small Computer System Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
IPV6	Internet Protocol Version 6
IPV4	Internet Protocol Version 4
DHCP	Dynamic Host Configuration Protocol (protocol for automating the configuration of computers that use TCP/IP)
VLAN	Virtual Local Area Network
SAN	Storage Area Network
PR	Persistent Reservations
SAS	Serial-Attached SCSI
FC	Fiber Channel
GUID	Globally Unique Identifier
GPT	GUID Partition Table
MBR	Master Boot Record
VSS	Volume Shadow Copy Service
CSA	Cluster Service Account
CNO	Cluster Name Object
AD	Active Directory
VCO	Virtual Computer Object
NTLM	NT LAN Manager
DNS	Domain Name Server

HP	Hewlett-Packard
RAM	Read Access Memory
MB	Megabyte
MPIO	Multipath Input/Output
I/O	Input/Output
NAS	Network Attached Storage
LUN	Logical Unit Number (SCSI devices)
NTFS	New Technology File System
ADDS	Active Directory Domain Services
CSV	Cluster Shared Volume
OS	Operating System
DVD	Digital Video Disc (now Digital Versatile Disc)
FTP	File Transfer Protocol
IIS	Internet Information Service
UPS	Uninterruptible Power Supply

1 INTRODUCTION

Organizations put a lot of value on business critical server and rely on them to be up and running all the time and provide business critical services whenever needed. A server with business critical services can cost thousands or tens of thousands when it is unavailable. This study was made to improve the server availability. Clustering is used to give high availability to the services that are clustered. In this study, the clustered component will be a virtual machine that means the whole operating system is highly available with all services in it. Virtual machine is software on physical hardware that executes instructions like a physical machine.

The clustering is used to improve availability fault tolerance. Clustering as a term means that several machines work together on defined purposes. Many of today's services that have a significant role in people's everyday lives are clustered in some way. For example the internet search provider Google has thousands of machines clustered to provide the search service to people.

The company that ordered the present study is Datapalvelut.net. Datapalvelut.net provides IT-services to small and medium size companies in the metropolitan area of Finland. Datapalvelut.net wanted to investigate possibilities to build a clustered server environment with low cost hardware equipment. The idea was to study whether it was possible to build a high available Windows Server environment with the low cost hardware. Also the question how it can be done is needed to be studied. The aim of the study was to work as a guide for Datapalvelut.net to build a regular high available server environment with low cost hardware.

This study differs from previous ones because in the study the hardware components are rather cheap and affordable by small businesses. Also the new feature cluster shared volume that came within Windows Server 2008 R2 failover clustering is compared to the previous storage model. Cluster shared volume is a cluster disk that can be accessed from every node for write and read operations simultaneously. Node is a machine which is a part of the cluster and will operate together with other nodes within the same cluster.

In the Study the experiments are explained in two parts. The first one introduces how the cluster was built and it also presents the instructions. The second part presents experiments that represent the most common failures in server environments. These common failures are based on the practical experience of the Datapalvelut.net organization.

The report is written in 5 sections. The first section introduces the features and properties of the Microsoft cluster service and clustering in general. The second section deals with the hardware devices that are used to build the environment for the study. The Third section gives the reader the possibility to build the similar environment as used in this study. The fourth section describes how this environment was experimented and why the experiments were done. The Fifth section presents the conclusions and results gotten from the experiments.

2 CLUSTERING SYSTEMS

This section introduces the clustering in general. The beginning of the computing cluster is briefly discussed and the main cluster types and minimum requirements are described. The Microsoft Cluster features are introduced in this section. Section includes a brief history of Microsoft Clustering and the benefits of the newest clustering feature that was included in Microsoft Windows Server 2008 R2.

2.1 Clustering History

Clustering is a group of independent servers that work together as a single unit. Clustering was developed to provide higher performance than a single server with low costs. Supercomputers provided a high level computing performance but they were very expensive.

Low Cost clustering was initially developed by two National Aeronautics and Space Administration (NASA) employees Donald Becker and Thomas Sterling, in 1993. In 1994 when Becker and Sterling were working under Center of Excellence in Space Data and Information Sciences (CESDIS) the cluster project named as Beowulf started. [1]

Since then the clustering has been researched to improve performance, availability, scalability and reliability. Organizations put a lot of value for high availability when the services that are clustered have an important role of the organizations business.

2.2 Clustering Basics

A cluster consists of server machines that are called nodes. The nodes need to have a Network Interface Card to be a part of the cluster. A network Interface Card is used to communicate between other nodes and System Area Network (SAN) in the same cluster. The performance of the cluster does not have any specific requirements although the performance of one node affects the general performance of the cluster. The node performance specifications need to be considered on the basis of the need from the cluster. System Area Network is a device where the actual clustered data resides. Data is accessible from all nodes at the same time or simultaneously. The storage system is vital within the cluster. The storage needs to have good

performance and reliable components on it. If there is only one storage system in the cluster it is a single point of failure. [2, chapter 2 & chapter 4]

A cluster can be built in multiple ways but there are still basic requirements for cluster. Firstly there are two machines that usually are server machines and those machines are connected together with one network connection called a heartbeat network. The heartbeat network is used for intercommunication between these nodes. The nodes send a health signal to each other in the heartbeat network. If the signal does not go through to the other node the node is then determined to be unreachable to the cluster and the tasks that are determined to happen in these situations will be executed. When there is an external source that needs to be connected to this kind of cluster there is a need to have a network device that can transfer the data to other network, for example Local Area Network (LAN) or Wide Area Network (WAN). Local Area Network is used when communication takes place inside one network that usually is an office local network. Wide Area Network is used when the cluster provides services over or to the World Wide Web (WWW).

There are basically two different methods of clustering, high availability clustering (HA) and Load-Balancing clustering (LB). High availability gives an opportunity to lose one of the hardware or software components and still the services that are clustered will work. This is used in business critical environments such as banking and stocking. High availability does only provide failover features so the performance is not increased. Even if there are more network objects the network is as fast as each component in it. Failover Clustering also provides transparent maintenance possibility for cluster nodes and components. Maintenance is done on clusters so that all services are migrated to another node in the cluster and the maintenance job is done when the node does not provide any services. Clients are not interrupted with the maintenance jobs and business critical applications are available all the time. After one node or component is ready from the maintenance operations other nodes in the same cluster can be maintained. [3]

Load-Balancing differs from the high availability with the way that it will provide multiple components to work together to achieve improved performance. In Load-Balancing cluster two network connections work together and the performance is twice compared to the single unit. Practical perfor-

mance is never doubled because the objects that control the Load-Balancing technique will decrease the performance with a small percentage. Load-balancing cluster is used when the services are highly populated or it will need a high performance from the hardware or software side. [3]

2.3 Evolution of Microsoft Clustering Service

Microsoft presented the first cluster service with Windows NT Server Enterprise Edition. The official name of the cluster service is Microsoft Cluster Server (MSCS) and the first version of that software feature was 1.0 codenamed ”Wolfpack”. Microsoft Cluster Server 1.0 was released in 1997 and since then Microsoft has offered Cluster Service Feature with Windows Server operation systems. [4, chapter 7]

Table 1 presents the maximum number of nodes in different versions of the Microsoft Cluster Service.

Table 1 Maximum number of nodes in one cluster of different Windows Operating System versions [5]

Operating System	**Number of nodes**	**Storage**
Windows NT 4.0 Enterprise Edition Windows 2000 Advanced Server Windows 2000 Datacenter Server Windows Server 2003, Enterprise Edition Windows Server 2003, Enterprise x64 Edition Windows Server 2003, Datacenter Edition Windows Server 2003, Datacenter x64 Edition	1-2	SCSI
Windows NT 4.0 Enterprise Edition Windows 2000 Advanced Server	1-2	Fibre Channel
Windows 2000 Datacenter Server	1-4	Fibre Channel
Windows Server 2003, Enterprise Edition Windows Server 2003, Enterprise x64 Edition Windows Server 2003, Enterprise Edition for Itanium-based Systems Windows Server 2003, Datacenter Edition Windows Server 2003, Datacenter x64 Edition Windows Server 2003, Datacenter Edition for Itanium-based Systems Windows Server 2008, Enterprise Edition Windows Server 2008, Enterprise Edition for Itanium-based Systems Windows Server 2008, Datacenter Edition Windows Server 2008, Datacenter Edition for Itanium-based Systems	1-8	Fibre Channel, iSCSI, or SAS
Windows Server 2008, Enterprise x64 Edition Windows Server 2008, Datacenter x64 Edition Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Datacenter Microsoft Hyper-V Server 2008 R2	1-16	Fibre Channel, iSCSI, or SAS

As Table 1 shows the nodes per one cluster have been doubled in all systems so that the cluster can provide a wider scale of configuration possibilities. Different configurations mean that different services can be configured to work with a specific number of the cluster nodes and other service will use other available nodes. This will improve the performance of the cluster when many services can be distributed within different nodes of the cluster. Also, the increased number of the nodes in one cluster will improve the availability with clustered services.

Table 2 lists possible resources that are supported by Microsoft Cluster Server in Windows NT Server. These resources can be clustered with two nodes. Both nodes can have any number of cluster groups that will include any number of resources configured for that group. Windows NT Server only limits the maximum number of nodes to two and those two nodes can cluster any number of resources. [6, chapter 1]

Table 2 Available resources in NT 4.0 cluster [6, Chapter 1]

Resource type, as listed in Cluster Administrator	**Description**
DHCP Server	Clustered installation of Microsoft Windows NT Server dynamic host configuration protocol (DHCP) servers
Distributed Transaction Coordinator	Clustered installation of Microsoft Distributed Transaction Coordinator (MS® DTC)
File Share	File shares accessible by a network path, such as *Servername**Sharename*
Generic Application	Network or desktop applications, such as a database program
IIS Virtual Root	Microsoft Internet Information Server (IIS) 3.0 (or later) virtual roots for WWW, FTP, and Gopher
IP Address	Internet Protocol network address
Microsoft Message Queue Server	Clustered installation of Microsoft Message Queue Server
Network Name	The virtual-server computer name for a network device or service
Physical Disk Print Spooler	Disk resources on the shared SCSI bus for shared folders or storage Printer queues for network-attached printers
Time Service	Special resource that maintains time consistency between cluster nodes

The range of resources that can be clustered is increased in every version and the Microsoft Server 2008 and Microsoft Server 2008 R2 have a Hyper-V resource in available. Hyper-V is a hypervisor-based virtualization system for x86 and x64 systems. Hyper-V virtualization brings a new aspect to the clustering and especially high availability.

Windows Cluster Server was renamed as failover cluster on Windows Server 2008 edition. In Windows 2008 The Quorum model has been changed from shared storage witness quorum to node and shared storage quorum model. In Windows Server 2008 the term Quorum refers to the majority of votes for which cluster node controls the cluster and cluster resources. By default, nodes and storages all get a vote in Windows Server 2008 failover clusters. Cluster can stay up as long as there is a majority of votes present. This can be a single node and shared storage, or both of the nodes without shared storage, in the case of a two-node cluster. On Windows Server 2003 the votes were given only to the nodes and this can be also configured to work such away in Windows Server 2008. There are four types of quorum models in Windows Server 2008. [8]

Node Majority: there is no file-share witness or disk witness and the votes are only assigned to nodes. More than 50 percent of the nodes must be available to make quorum. Figure 1 shows an example of a Node-Majority quorum.

Figure 1 Node Majority Quorum Model

Node and Disk Majority: Nodes and a shared disk get votes. This configuration allows a loss of half the nodes, providing the disk witness is available, or over half the nodes are available without the disk witness being available. Figure 2 shows an example of a Node-and-Disk-Majority quorum.

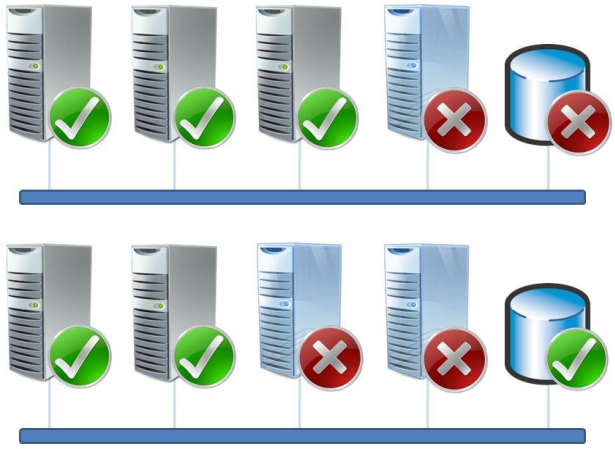

Figure 2 Node and Disk Majority Quorum Model

Node and File Share Majority: The same as Node and Disk Majority, except the shared disk is replaced with a file-share witness. Figure 3 shows an example of a Node-and-File-Share-Majority quorum.

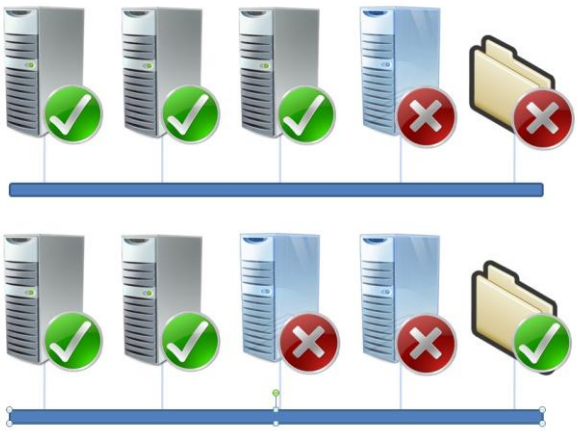

Figure 3 Node and File Share Majority Quorum Model

No Majority: Disk only: The disk witness must be available to have quorum, but the number of available nodes does not matter. Figure 4 shows how the disk witness must be available to have quorum.

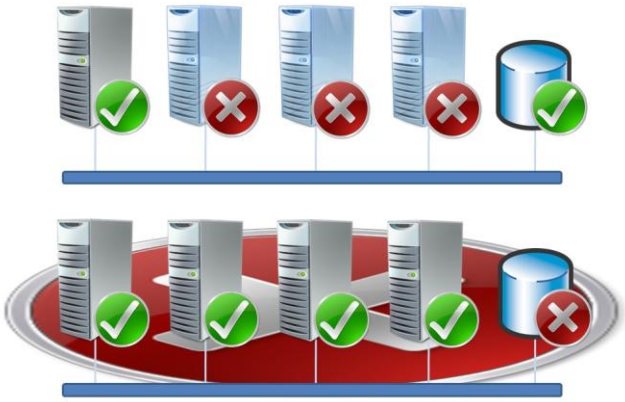

Figure 4 No Majority: Disk Only Quorum Model

The figures above illustrate the quorum models. The quorum models are in a vital role when the cluster is planned. The intention of the figures is to help the reader to imagine the quorum models with the hardware components.

2.4 Failover Clustering on Windows Server 2008 and Windows Server 2008 R2

Microsoft Windows Server 2008 provides failover clustering feature with improved architecture when compared to the clustering feature in Windows Server 2003. Windows Server 2008 supports more nodes than before. There can be 16 nodes in one cluster compared to the 8 that is the maximum number of nodes in Windows Server 2003. Also the networking model and, to be more specific, the heartbeat process is changed from the broadcast to the unicast. With this improvement nodes can be located from different locations, subnets and behind different network routes. Cluster nodes can transmit the heartbeat signal in the local area network or the iSCSI network. This will release one more network adapter to be configured to these networks to provide better fault tolerance for the network. [8]

The maintenance mode is changed so that when one node is in maintenance mode the health checking is disabled on that node. This was failing the cluster nodes in previous cluster service versions because the maintenance mode gave errors to the cluster. [8]

Windows Server 2008 Failover clustering supports Ipv6 addresses. That gives the opportunity to have globally more IP addresses because the length of Ipv6 address is now 128 bits when Ipv4 addresses have 32 bits. Windows Server 2008 supports DHCP addressing as Windows Server 2003 uses only static IP addressing. DHCP can be determined as per-interface so if one in-

terface uses DHCP then it will only allow DHCP addresses. These features provide more flexible administering on clusters. There is no need to configure VLANs across WAN anymore because cluster nodes can be in different subnets. [8]

A new Quorum model is provided with Windows Server 2008, Majority Quorum Model, described in section 2.3.

Windows Server 2008 failover clusters are designed for SANs. Only persistent reservations (PR) SCSI commands to the disk are supported. Most commonly used SAN bus types are supported, such as Serial Attached SCSI (SAS), Fiber Channel (FC) and iSCSI. The handling of cluster disks is moved to the windows Disk Management service. And the GUID partition table (GPT) disks are now supported which improves the capacity of one partition to be over 2 Terabytes and the primary partition limit is increased to 128 as it is in MBR only 4 (3 primary partitions and an extended partition). Windows Server 2008 has added support for VSS backup as it has its own VSS writer and the clustered applications backups are simplified. [8]

Obviously security is a prerequisite in any organization IT infrastructure and it has been improved in failover cluster service in Windows Server 2008. Cluster service configuration in Windows Server 2003 is under Domain user account called Cluster Service Account (CSA). In Windows Server 2008 cluster service runs under a local administrator account which has the same privileges as cluster service account. This account relies on the Cluster Name Object (CNO) that is created in Active Directory (AD) when a cluster is created. CNO is used to create Virtual Computer Object (VCO) when a network names are created and brought to online. [8]

Primary authentication is changed from Legacy NT LAN Manager (NTLM) to the Kerberos authentication. All communication between nodes are secure, encrypted inter-node communication is still configurable. [8]

Windows Server 2008 R2 brought a new type of storage usage to the failover cluster when Hyper-V is used. That storage type is cluster shared storage. Cluster shared storage differs from host-based storage in that all nodes of the cluster will have access to the cluster shared storage simultaneously. All write requests are sent to one node which will control the cluster shared volume. Only one node can write to the cluster shared storage at a time.

Host-based storage is always attached to only one node at the time and when the write access needs to be changed the ownership of the storage needs to be changed. Cluster shared storage provides easier maintenance of the cluster storages and multiple virtual machines can be installed on one LUN disk. Disk labels are not anymore limiting the maximum number of possible virtual machine in the cluster. Cluster shared volume creates a shared folder on all nodes which is located on the system drive root and folder is named as ClusterStorage. [9]

3 TESTING ENVIRONMENT AND METHOD

This chapter is to introduce the hardware needed in building the server, network devices and the storage device. The second part of the chapter describes how to build an infrastructure similar to the one used in the present study.

3.1 Hardware Equipment

This section describes the equipment used to build high available Hyper-V environment. The section is divided into three parts. The first section discusses server hardware, the second section with network devices and the third section introduces the storage device information.

3.1.1 Server

HP Proliant DL 320 G6 is used as primary server hardware in the experiments. HP Proliant DL 320 G6 is a low cost rack-optimized server. The server has 1 unit deep chassis, 1 Intel Xeon 5600 series processor and 8 gigabytes of memory. The unit used in this study has an additional network card installed. The network card that is used is HP NC360T PCIe Dual-port Gigabit server adapter. The server unit chassis is shown in Figure 5. [10]

Figure 5 Hewlett Packard Proliant DL 320 G6 Server [9]

Another server that is used in this study is HP Proliant ML 110 G4. Proliant ML 110 G4 is used as a secondary server that is planned to be used only when the main server DL 320 is unavailable. This is one way of saving money when the costs of hardware equipment can be reduced when using cheaper backup nodes. Reliability can be still improved when the all nodes have reliable components that are mirrored on the hardware case. Power components should be mirrored so that if one power supply unit fails the other is used automatically without interrupting the operations of the server. Proliant ML110 G4 has different processor architecture than Proliant ML320 G6. This will be noticed in the section 3.2.5 when environment was build. Proliant ML110 G4 has an Intel Xeon 3050 processor, 4 Gigabytes of RAM and also an additional network card that is the same as in Proliant DL320 G6 server. The network card needs to be the same because the clustered virtual network is built on it. Figure 6 shows the server chassis and as can be seen the server is tower model server. [11]

Figure 6 Hewlett Packard Proliant ML 110 G4 Server [10]

Both of the servers used in the experiments are second hand servers and there are additional memory installed to the servers.

3.1.2 Network

Local Area Network is built with a basic consumer router Zyxel NGB-417N. This router only acts as a DHCP server and routes the network traffic to the right directions. This router can provide only 100 MB Ethernet connection and it is used to provide the local area network of the environment. The default configuration is used in this study.

Figure 7 Zyxel NGB-417N Wireless Router

The iSCSI network is built with two Zyxel ES-108A switches. These switches can provide only 10 MB or 100 MB network connection and those will not provide the best performance for the iSCSI network. It is suggested from the Microsoft that iSCSI network is built with 1000 MB switches and network adapters. In this study, the performance of the environment does not have an important role and it can be improved with similar switches that can offer 1000 MB connection. There are two switches used to provide high availability routes to the storage system. The iSCSI switches used in the experiments are illustrated in figure 8.

Figure 8 Zyxel ES-108A Ethernet Switch

The router and the switches used are meant for consumer environments and the performance and reliability can be improved when high-end devices are used.

3.1.3 Storage

The most important hardware equipment in a cluster environment is the storage system. There is a huge collection of different kind of storage systems that can be used when clustered services are needed. The provided features that will improve the performance and reliability of the cluster in this storage device are SCSI-3 Persistence and Multipath I/O connections. These features need to be supported by the storage system In Windows Server 2008 the failover clustering. The storage device used in the experiments is illustrated in Figure 9.

Figure 9 QNAP TS-239 PRO II Storage System

In this study the storage device used is a QNAP TS-239 PRO II with two Western Digital 750 GB hard drives installed. QNAP TS-239 PRO II provides the iSCSI storages to the cluster. The storage has two network adapters in the storage server.

3.2 Building Failover Cluster Environment

This section gives information on how to build a similar infrastructure as used in this study. The Failover Cluster can be configured in many ways and the configuration depends on the purpose of the cluster. In this study the cluster is configured with basic configuration to answer the question made by Datapalvelut.net.

3.2.1 Pre-installation of Software

Both servers need to have at least Microsoft Windows Server 2008 Enterprise version that supports failover clustering features. The installation of the Windows 2008 R2 Enterprise Edition is made on both servers. After having done the installation on both servers, more specified configurations are always needed. These are described in following sections. There are no special requirements on behalf of the failover cluster on the raid versioning, hard

drive partitions or locations. In this study there were raid level 1 configured on the hard drives in both servers.

Storage is preconfigured with the QNAPs installation tool. The software called QNAP Finder was used to find out the given IP address from the DHCP. The software is shown in Figure 10 and it is downloadable on the QNAP website (http://www.qnap.com). The Quick configuration will determine all necessary configurations to the QNAP storage system. These configurations include naming the storage, giving static IP addresses, configuring the hard drives installed and the supported features of the devices. After the quick configuration has been done the network connection must be set to the failover mode from the network configuration tab under the system configuration. System configurations are accessible with web browser when the IP address of the QNAP is entered.

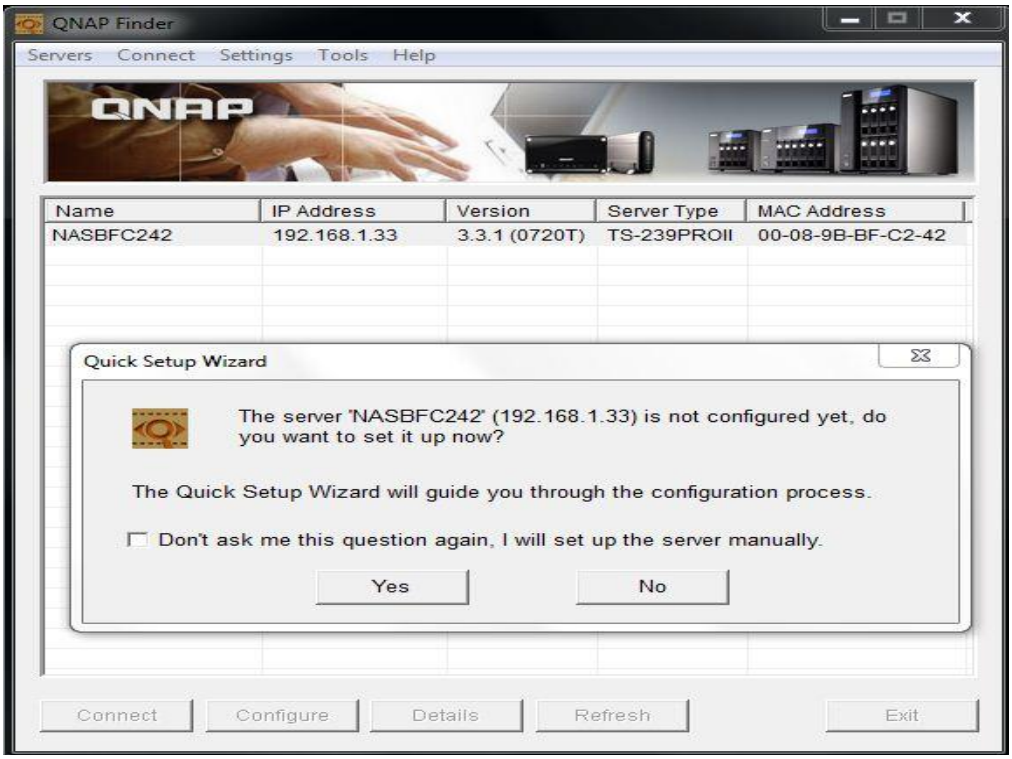

Figure 10 QNAP Finder Software

After the Windows servers were installed the name was changed on both servers. Names were given so that the main server which is Proliant DL320 was named as node1 and the Proliant DL110 was named as node2. After the names were given on the servers the next thing was to configure the

network adapters of the server. The network configurations are explained in the next section.

3.2.2 Network Configurations

Network configuration has an important role in the failover cluster. The connections should be planned to have a backup route for every network and if one cable fails the other will still provide the connection. In this study the network configuration was limited from the Proliant DL110 side because there were only 3 network adapters available. There were two HP 1 gigabyte network adapters and one Broadcom 1 gigabyte adapter. Proliant DL320 has 4 network adapters, 2 HP 1gigabyte and 2 Broadcom 1gigabyte. The network adapters on the cluster environment need to match with other network adapters on each server. The configuration was made so that 1 Broadcom adapter was used to provide LAN connections to the servers and the Hyper-V virtual network was configured to work with that adapter. 2 HP adapters were used for the iSCSI network connections to provide a failover possibility to the iSCSI network.

The local area network was configured to have 192.168.1.0 /24 and the iSCSI network to 10.0.0.0 /24 networks. The server named as node1 was configured with local area network IP address of 192.168.1.10. And iSCSI network addresses of 10.0.0.10 and 10.0.0.20. Another node named as node2 was configured with local area network IP address of 192.168.1.20 and iSCSI network addresses 10.0.0.30 and 10.0.0.40. The storage system was configured to use 10.0.0.50 IP address on the iSCSI network. Local Area Network does not have access to and from the QNAP so the iSCSI IP address was the only to be configured to the QNAP storage.

After the physical adapters were configured on the both server nodes and the QNAP storage system the Hyper-V network needs to be built. Virtual network manager for Hyper-V is included to the Hyper-V manager. From there the virtual local area network switch is built. Hyper-V virtual switch shares the one physical adapter to the virtual machines through the virtual switch as the Figure 11 shows below.

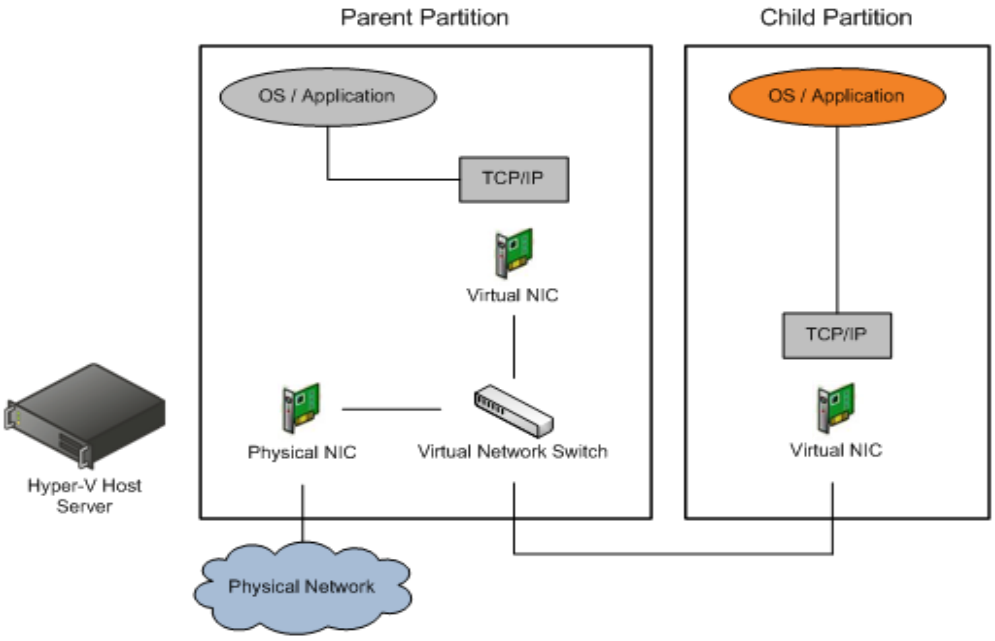

Figure 11 Physical Network Card Configuration As Virtual Network Card

Hyper-V virtual network was configured through the Hyper-V manager and from there the Broadcom network adapter was chosen for the use of virtual Local area network. The virtual network must be configured to be an external connection so other devices on the local area network can connect to the virtual machine using only this virtual network. The configuration window is shown in Figure 12 below.

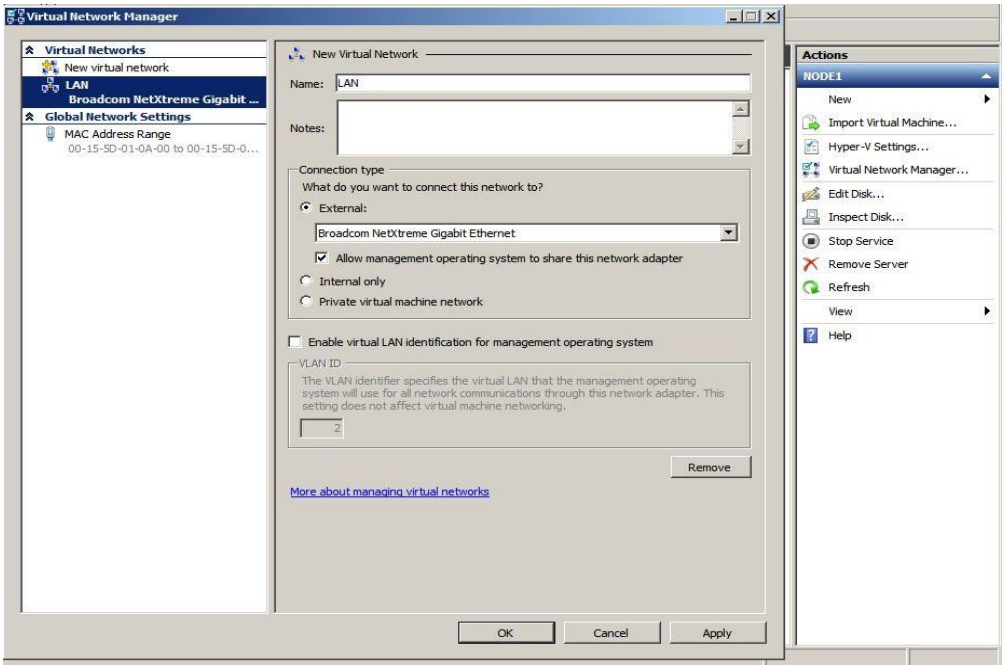

Figure 12 Hyper-V Virtual Network Manager Configurations

The configurations were made on physical node servers, QNAP storage system and Hyper-V virtual network. The next thing was to make the cabling between the components. The iSCSI network was built from the HP network adapters through two different switches to the QNAP storage. The connections were made from one node to both switches so that if one switch or cable will fail the other switch can still provide connection from the nodes to the storage system. This prevents the single point of failure for the switch component. The network diagram is shown in the Figure 13.

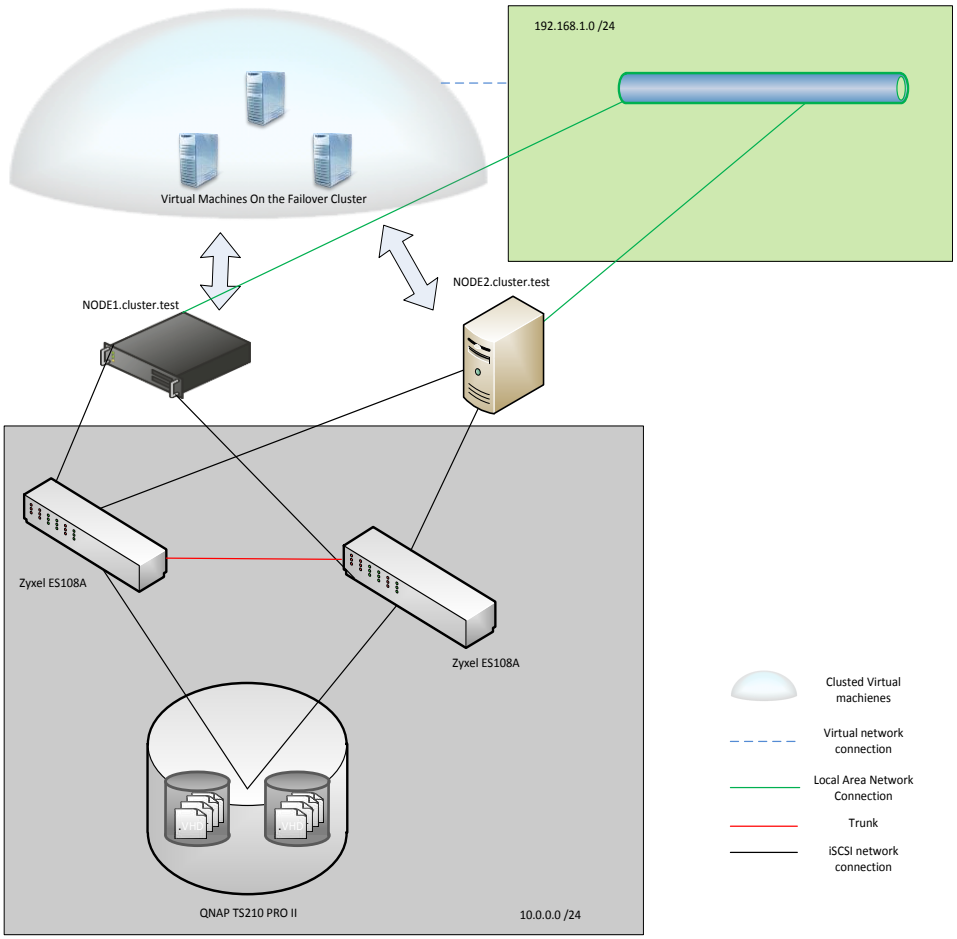

Figure 13 Graphical View of the Environment

As illustrated in Figure 13, the QNAP storage is a single point of failure. The QNAP has two hard drives and two network connections but the unit itself may fail and the whole cluster is then unavailable. Also the LAN connections have only one route from each node so if the adapter or the cable fails the clients cannot reach the services provided from the cluster. The services will be online but not accessible from the LAN. Suggested improvements of the environment discussed in Section 6.

3.2.3 Storage Configurations

Storage connections were made with iSCSI initiators and the QNAP will provide the LUNs to the node. In this study there were both cluster shared volume and host-based storage LUNs configured to the QNAP. This was configured both ways only for comparing the differences between these two cluster storage styles. iSCSI targets were configured from the QNAP web site administration panel. iSCSI settings can be found under disk management and there is an iSCSI sheet where the configurations are made. iSCSI configuration panel is shown in Figure 14. On the figure all necessary iSCSI targets and LUNs were already configured and ready to be connected.

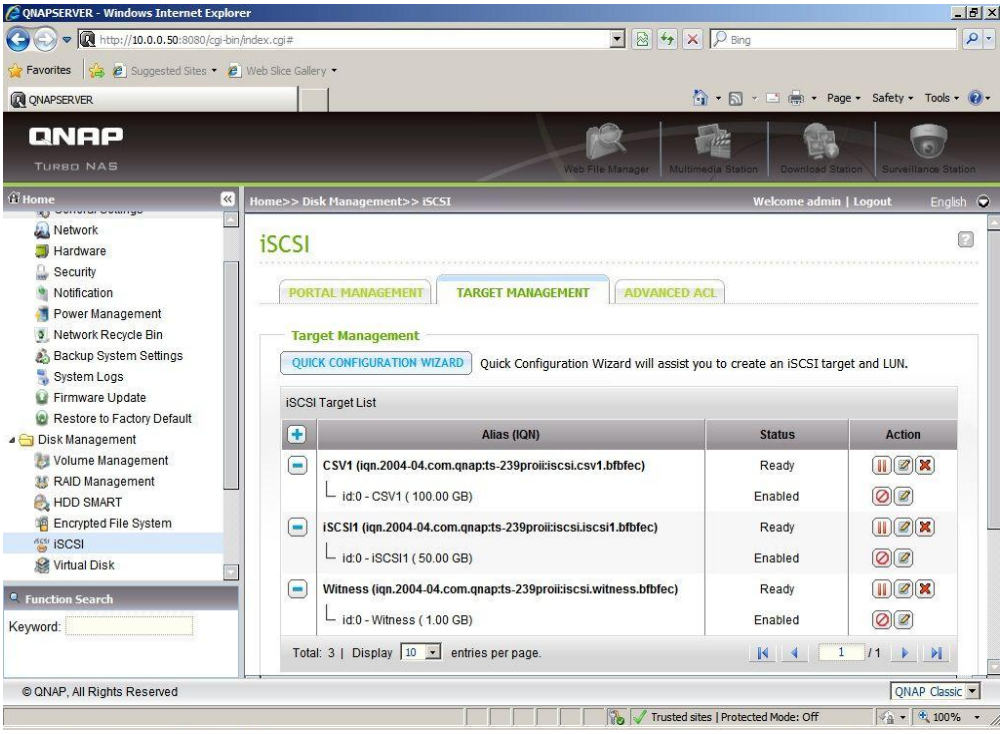

Figure 14 QNAP Storage Systems iSCSI Configurations

After all iSCSI targets and LUNs are configured and they are in ready state on the QNAP, the LUNs can be targeted to the node servers. It is done with the iSCSI initiator service from the Windows Server 2008 R2. iSCSI initiator service is disabled by default and it can be enabled from the administrative tools where the the iSCSI initiator needs to be chosen. After the iSCSI initiator is chosen to be enabled, the QNAPs IP address is entered to the quick connect field. The configured iSCSI targets will appear to the iSCSI initiator favorites list as shown in Figure 15. All iSCSI connections are configured to use multipath. The multipath requires two sessions to the iSCSI target. This

is done by choosing the properties of the iSCSI target and there one more session is added with multipath enabled. In Figure 15 the iSCSI targets were already connected and all connections have two sessions with multipath enabled.

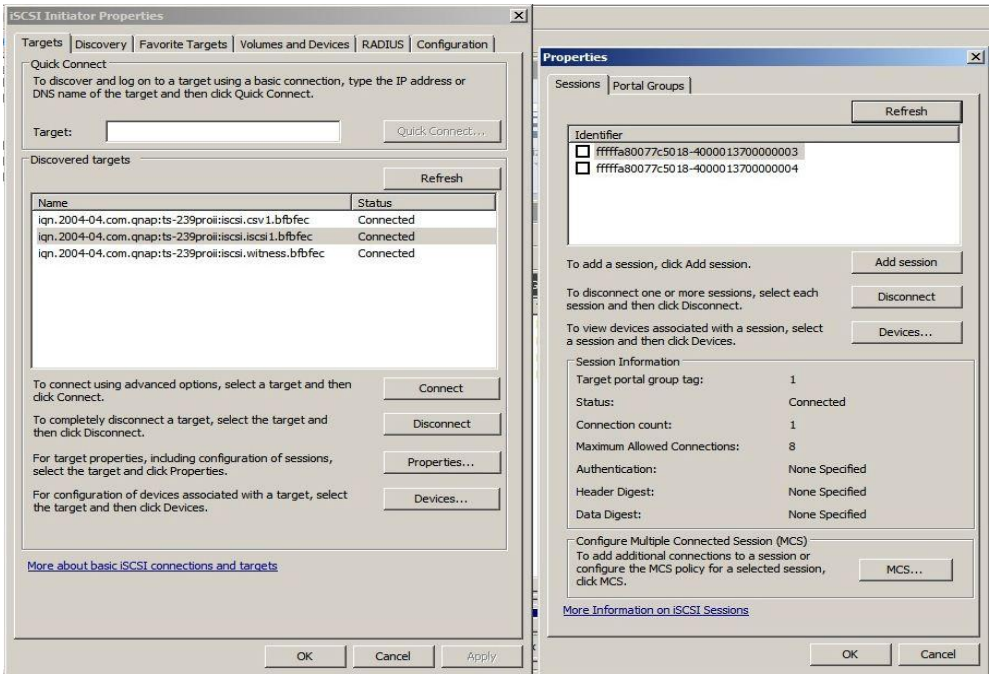

Figure 15 iSCSI Target Configurations

When iSCSI targets are connected and configured the LUNs will appear to the server's disk management configuration panel in the server manager windows. This is shown in Figure 16 where all three iSCSI LUNs were already listed in the disk management panel.

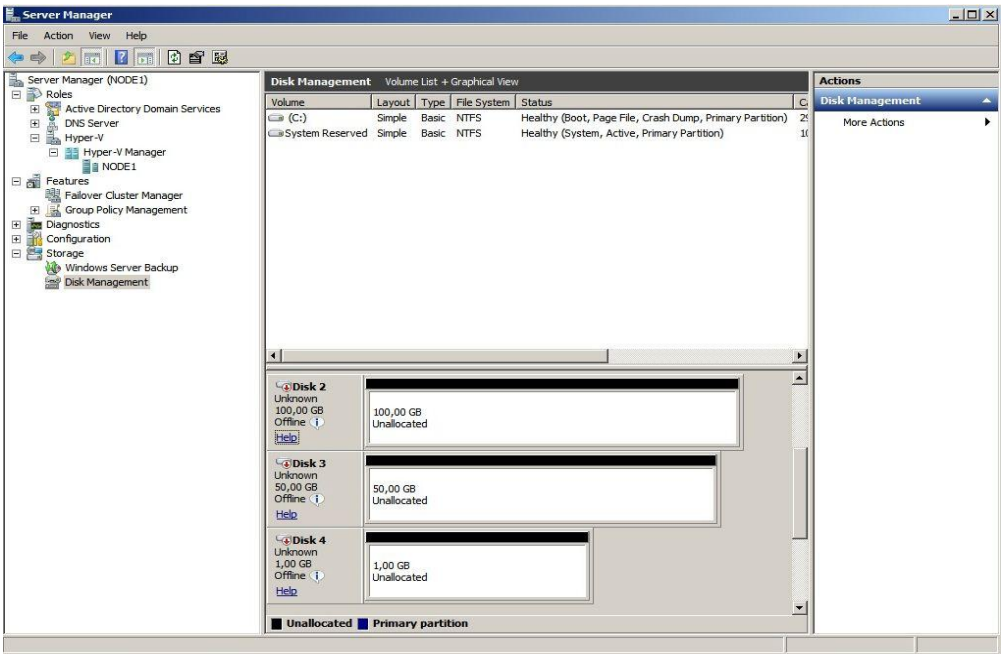

Figure 16 Disk Management View before Disk Partitioning

These new hard drives need to be taken to the online state from one of the nodes. After the hard drives are online, initialized and formatted with NTFS partition they can be used as physical drives from the server. These drives are now operational and can be found as a physical disk on the server as shown in Figure 17.

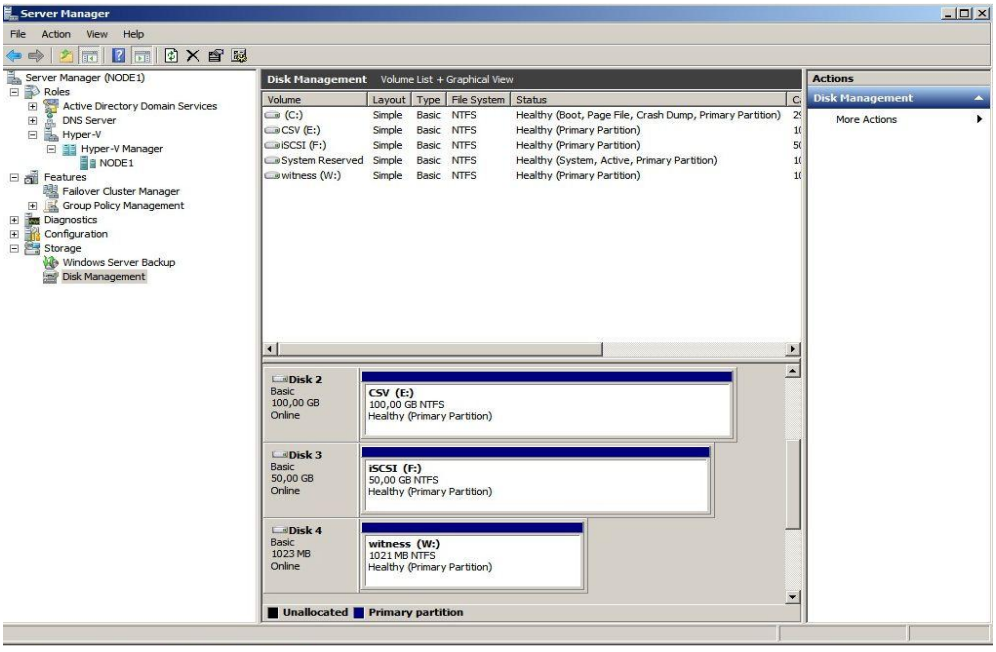

Figure 17 iSCSI LUNs Taken Online on Node Server

After iSCSI LUNs are configured with the multipath and they have a NTFS partition they need to be connected also to all other nodes in the cluster in the similar way. In other nodes the disks need to be taken to the online state and the initializations and partitioning from the other servers is no longer needed. The cluster validation tool tests the hard drives that are compatible to be used in the cluster and this is the reason why all nodes need the connections to be configured. When LUNs are connected, the Multipath I/O needs to be configured to the disks. From the disk management panel the properties of the LUN disks are chosen. It will open window called QNAP properties and there is MPIO tab where the MPIO policy is chosen to be as Fail Over only as shown in Figure 18.

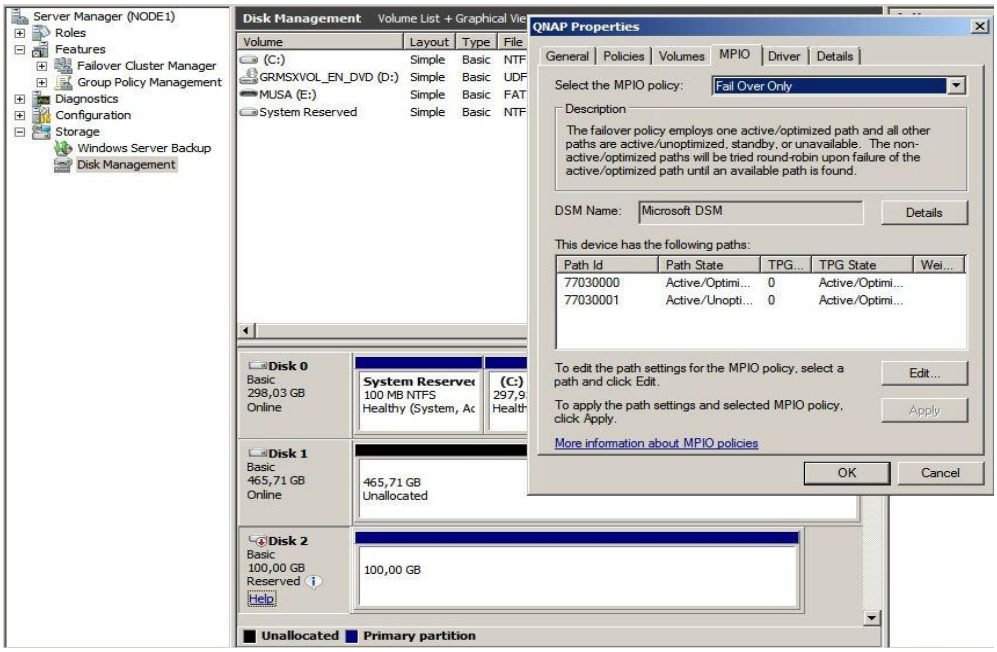

Figure 18 Multipath Configurations with Fail Over Only Policy

When the multipath was configured to the disks all settings to the storages were done excluding the cluster storage configurations which are explained in the following section.

3.2.4 Failover Cluster Feature Configurations

Failover clustering service requires Active Directory account to manage the cluster configurations. Both nodes are configured to be Active Directory Domain Controllers. After Windows Server 2008 R2 installation was made the role Active Directory Domain Services can be installed on both nodes. Active Directory Domain Services can be installed on roles sheet of the server

management windows and there the add roles option is chosen. After the roles are installed, the Active Directory needs to be configured with the dcpromo.exe command. In this study the server named as node1 was configured to create a domain called cluster.test and node1 was configured to be domain controller on that specific domain. Both nodes should be configured as global catalog server and also the DNS server role needs to be installed with dcpromo tool. When the domain is created the node2 needs to have an Active Directory role also and that server is joined to the existing domain cluster.test with dcpromo tool.

Both node servers will need also Hyper-V role, Failover Clustering and Multipath I/O features. These features can be installed from the server manager window by right clicking on the features and in there the selection, add features are chosen.

Hyper-V role was installed because in the experiments the failover clustering was used to provide highly available virtual machines. Figure 19 shows the roles and features excluding multipath I/O feature which need to be installed.

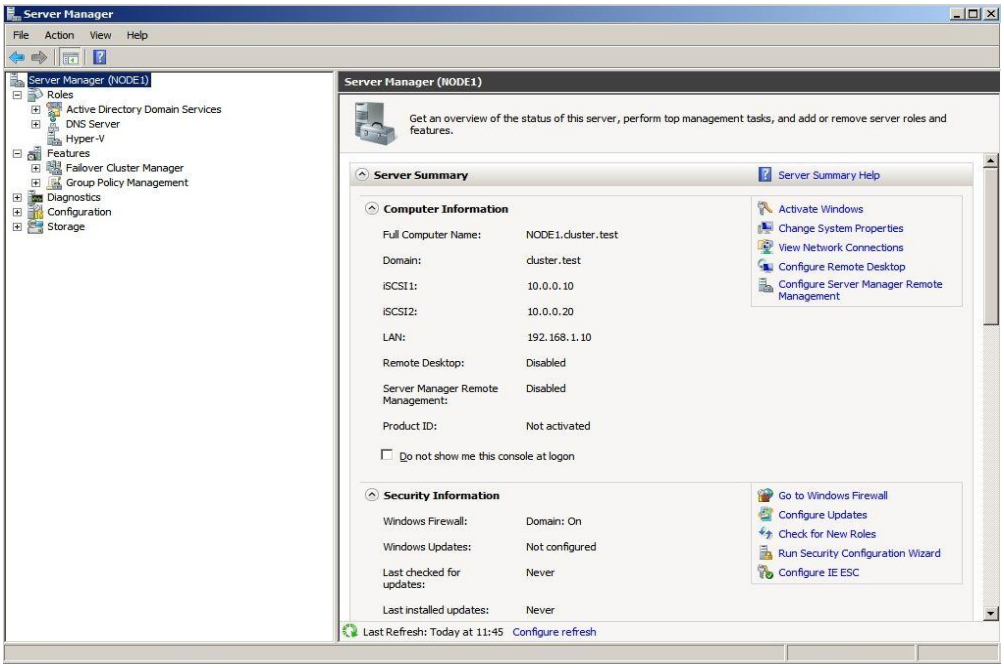

Figure 19 Server Roles and Features

The next step is to validate and create the two node cluster. When failover cluster manager is chosen from the server manager window the validation is made to validate the cluster components and configurations on the servers.

Validation starts by entering the nodes that will take part in the cluster and there will be chosen both servers node1 and node2 as shown in Figure 20.

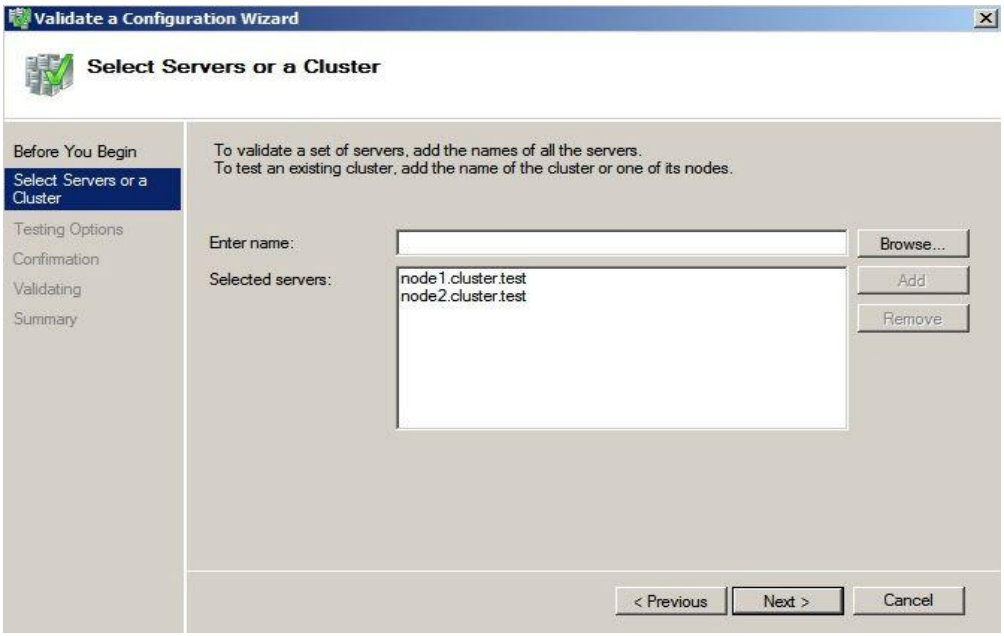

Figure 20 Cluster Validation Tool Servers Listed

The validation tool allows the user to choose only specific tests which are tested. This is very useful when there is only one part of the configuration changed. For example one broken network adapter is changed to another working one and the configuration is made again on that adapter. This replacement can be validated with this tool when choosing to test only network configuration. The validation process informs if there are any components or configurations that are not supported by failover clustering. When the cluster is created for the first time all tests are chosen to see that the cluster is correctly configured. Figures 21 and 22 illustrate the validation tool process that is included in the cluster configuration wizard.

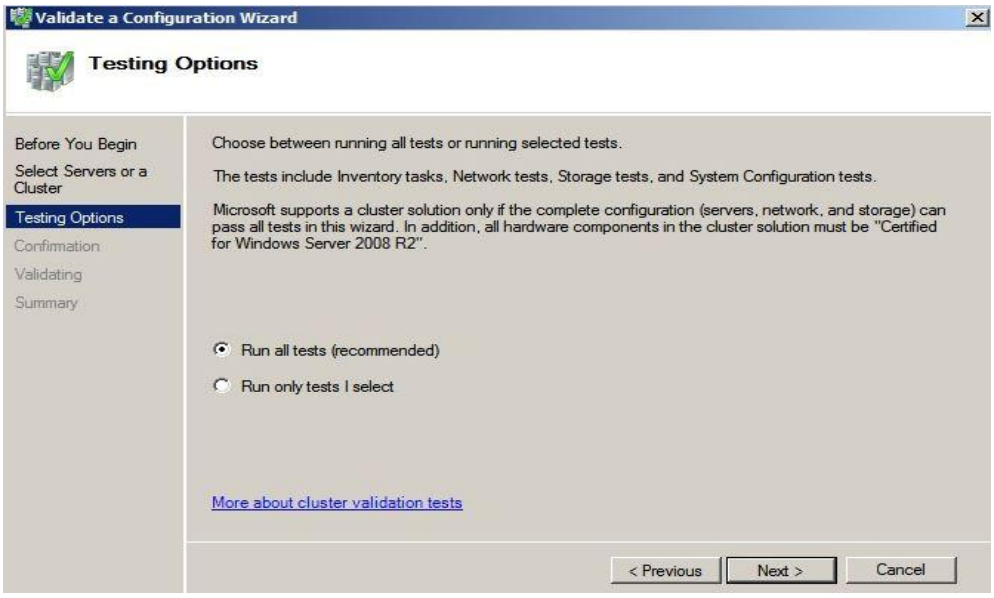

Figure 21 Validation Tool Tests Selection Page

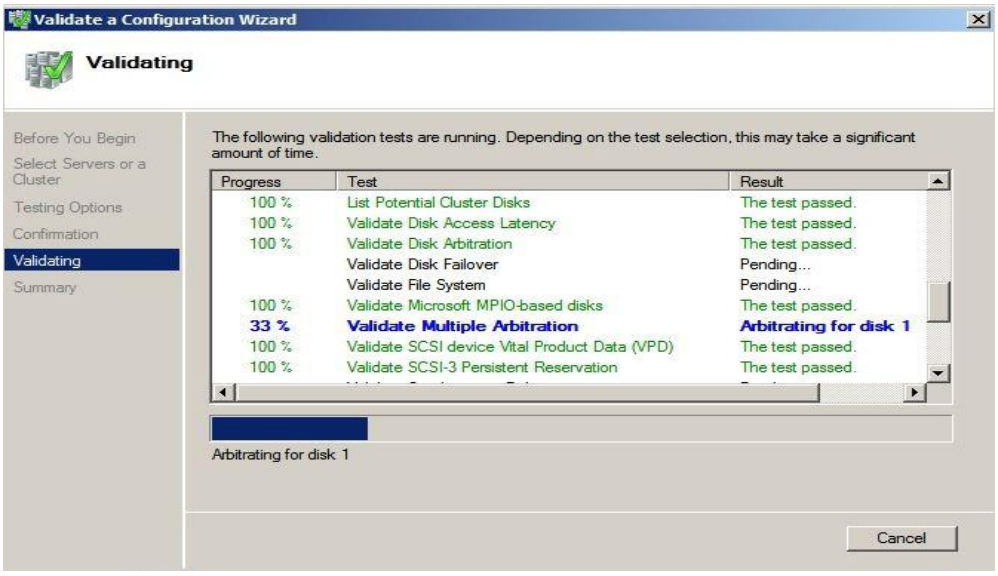

Figure 22 Validation Tool Validating Tests

As Figures 21 and 22 illustrates the all tests was chosen to be run. In Figure 22 all tests that are shown in the figure are passed. If any feature is not supported by the validation test the specific test itself will be shown with red color. After validation tests have been run through the cluster can be created. When a cluster is created there is a need to define a cluster name. The Cluster name is an Active Directory component that clients use to connect highly available services. In this study all experiments were made with Hyper-V virtual machines so the name of the cluster actually did not matter at this point. Hyper-V does not use cluster name objects for connections because all connections were made straight to the virtual machines operating

system. Even though there is no need to give a name to the cluster it has be to given some name and the cluster was named *hypervcluster*. The Cluster also needs an IP address and the address was determined to be on LAN side so that LAN clients can connect to the cluster. The IP address was configured to have an IP address 192.168.1.100. These configurations are shown on Figure 23.

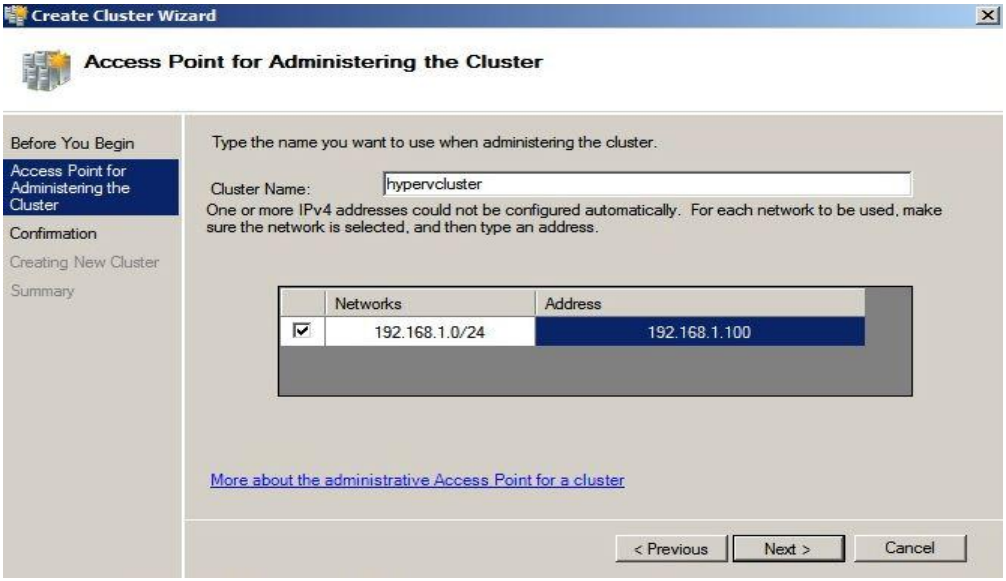

Figure 23 Cluster Name Configuration

Failover cluster automatically makes a Quorum model to be a node and disk majority when using similar configurations as this was made. The quorum model was left as it was because it will provide the best availability to the cluster when having only two nodes and one storage device. Cluster storage disks are also automatically generated after validation and cluster creating process is done. The Cluster shared volumes were needed in this experiment so it was necessary to set this available for the cluster. Cluster shared volumes can be set available in the cluster management console by right-clicking the cluster name and in there is an option to enable cluster shared volumes. After cluster shared volumes were enabled one storage was added to the cluster shared volume storage and that is 100 GB LUN called CSV that is already made to the QNAP.

At this point the failover cluster was configured and working. There were no services specified to have high availability feature. The next section introduces the configuration of the Hyper-V virtual machine to be high available.

3.2.5 Configure Hyper-V Virtual Machine with High Availability

The Hyper-V virtual machine was configured to use a cluster shared volume. This means that the operation system partition of the virtual machine is configured to locate on the cluster shared volume. In the failover cluster manager under the services and applications part there can be found a virtual machine selection. In the virtual machine selection the new virtual machine was chosen and the new virtual machine was pointed to one of the nodes, in this case it was built on the node1 server. The Virtual machine creating option is illustrated in Figure 24.

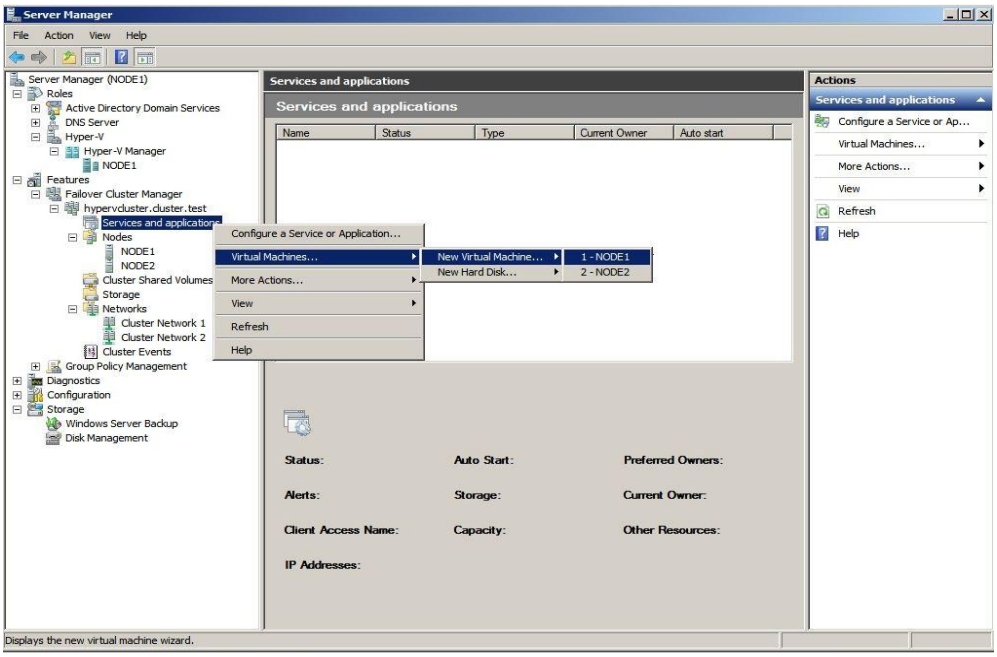

Figure 24 Installing New Hyper-V Virtual Machine

When the new virtual machine wizard configuration window is opened the virtual machine name and configuration file location was to be determined. The virtual machine was named as CSV_VM and the location was cluster shared volume location which is in c:\clusterstorage\volume1 path. The first part of the configuration of the Hyper-V virtual machine is shown in Figure 25.

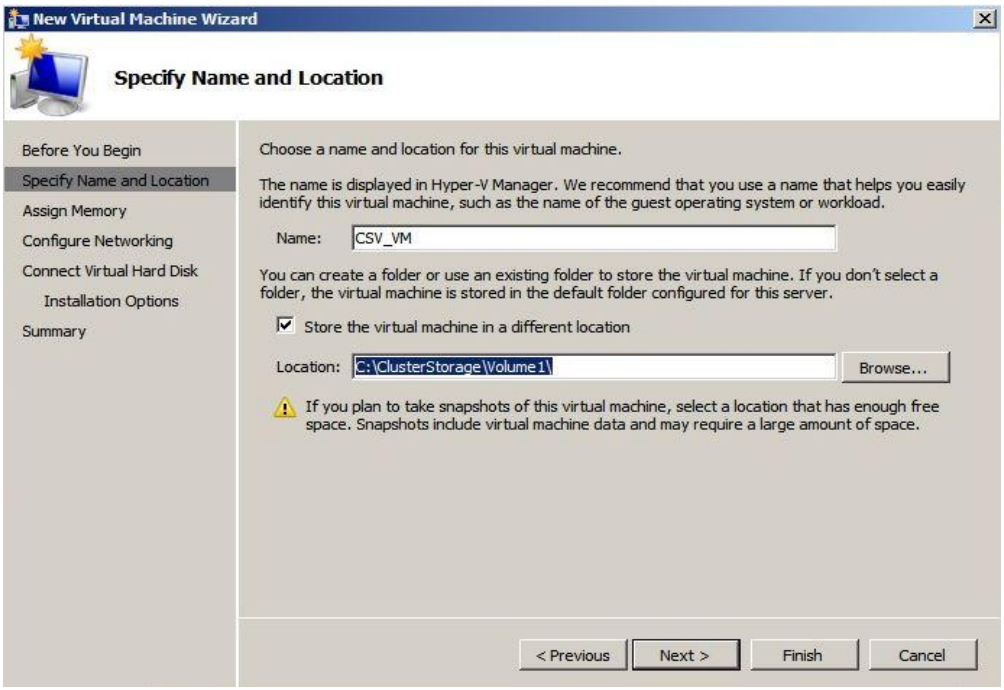

Figure 25 Hyper-V Virtual Machine Configuration Page 1

The next part of the wizard is to determine the amount of RAM given to the virtual machine. The RAM amount needs to be the amount that will always be available on both nodes. If there are more than one virtual machine the lowest amount in one node of RAM is divided between the virtual machines. This is done because if one node fails all virtual machines failover to another node and there must be enough physical RAM on the node so that it can virtualize the total amount of RAM for all virtual machines. If the physical RAM is not available the virtual machine will not automatically startup after failover occurs.

CSV_VM virtual machine was configured to use only 1500 MB of RAM, as shown in Figure 26. This should be available all the time because the proliant DL 320 has 8 gigabytes and proliant dl 110 has 4 gigabytes of the total RAM capacity.

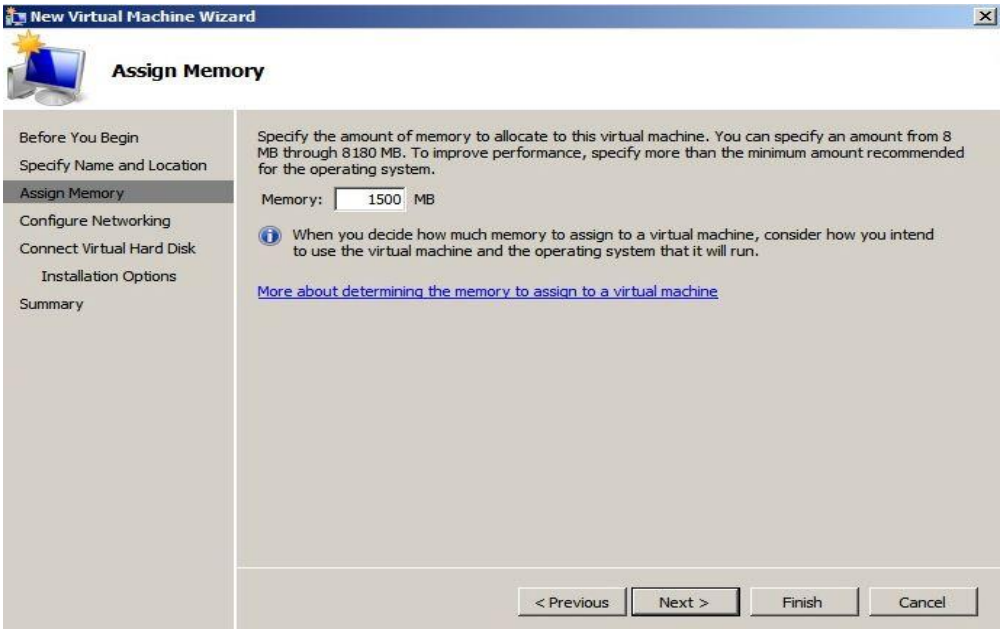

Figure 26 Hyper-V Virtual Machine Configuration Page 2

The network connections were configured to use already configured virtual network named as LAN, the network configuration is shown in Figure 27. This will provide connectivity from the LAN users to the virtual machine and vice versa.

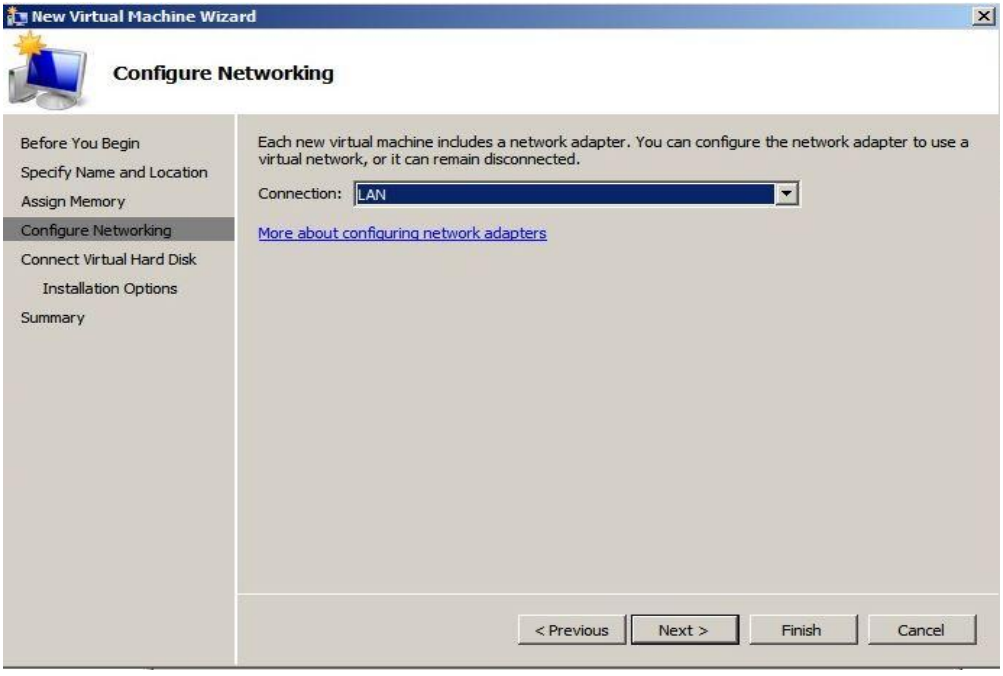

Figure 27 Hyper-V Virtual Machine Configuration Page 3

The hard drive of the virtual machine was needed to be configured to the clusterstorage folder which is the cluster shared volume location of the failover cluster. CSV LUN on the QNAP was configured to have a maximum size of 100 GB so the virtual hard disk was determined to be of the same size. Virtual hard drive configuration is shown in Figure 28.

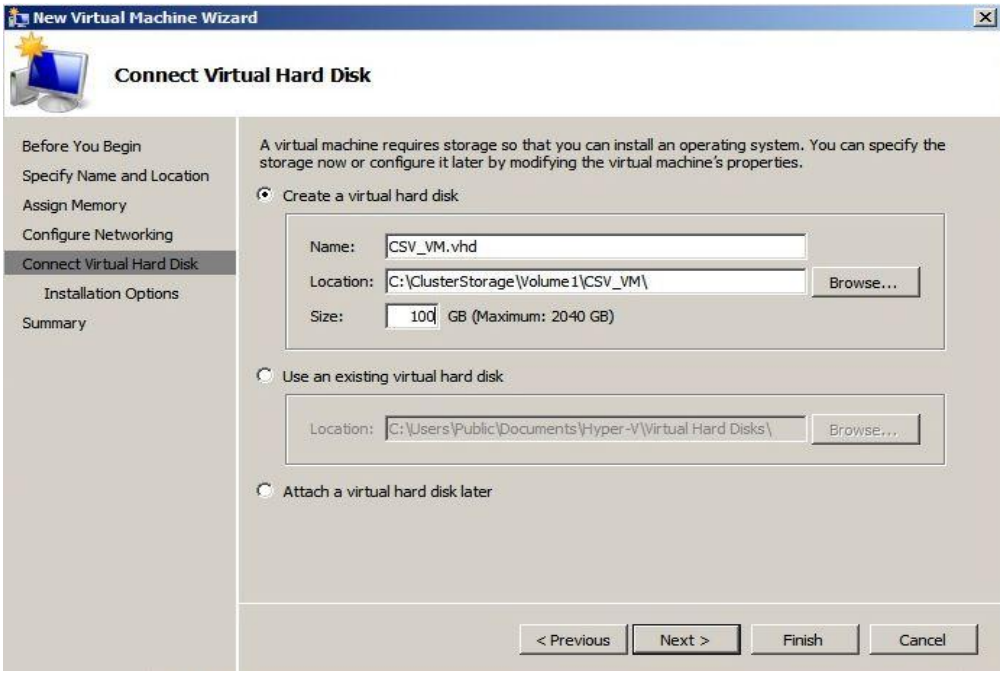

Figure 28 Hyper-V Virtual Machine Configuration Page 4

Also the location of the Operating System installation software needs to be determined on the wizard. In the present study the operation system was installed from the DVD and therefore a physical DVD drive of the node1 server was chosen to be used as an installation source.

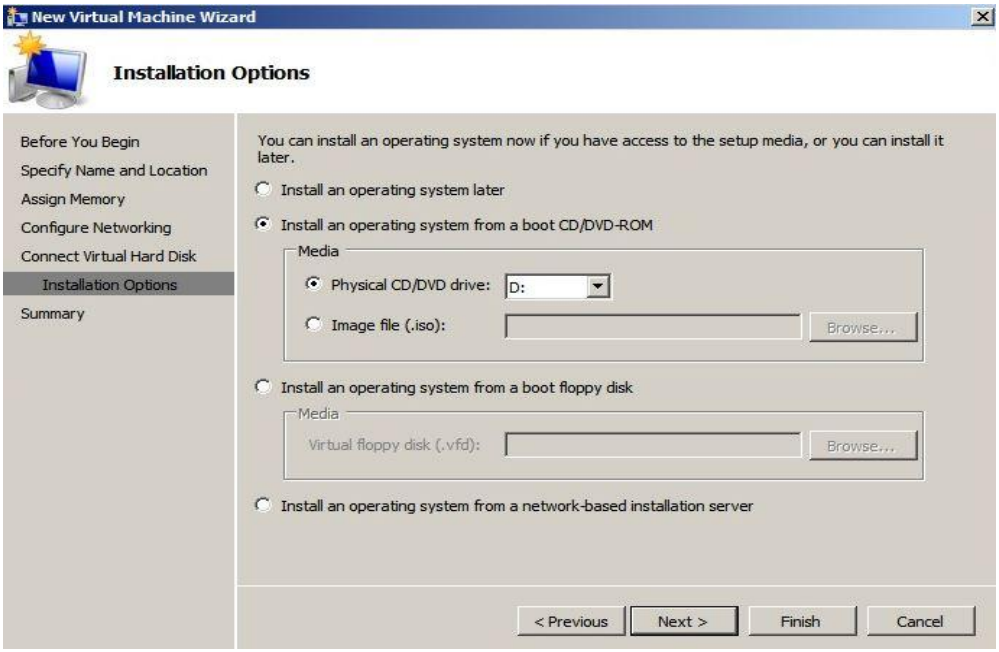

Figure 29 Hyper-V Virtual Machine Configuration Page 5

At this point the virtual machine has all necessary configurations made so that it can be started on the clustered node server and the operating system can be installed. The Hyper-V virtual machine was now shown under the services and applications on the failover cluster manager. This means that the virtual machine named as CSV_VM was configured to be high available in the cluster. The operation system was installed on the virtual machine for test purposes.

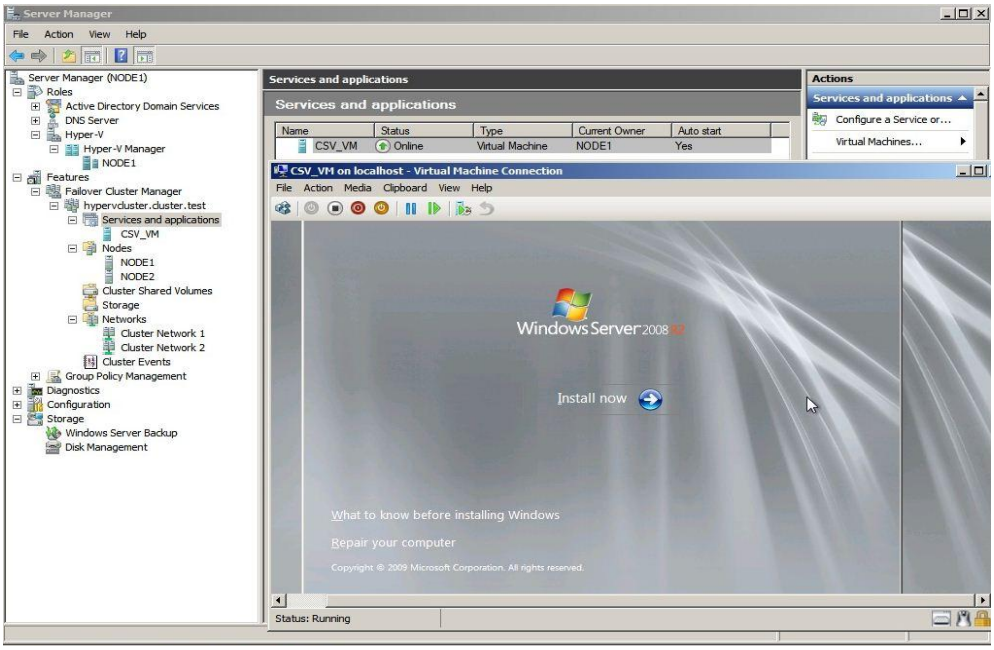

Figure 30 Installing Operating System on Clustered Virtual Machine

After the operating system was installed there were a couple of changes to do with the virtual machine before it can really be high available on this environment. The first change was to take the physical DVD drive offline from the virtual machine because this physical DVD was not identical with another node and it cannot be migrated to another node. The physical DVD can be detached from the virtual machine settings. Another change was to enable migration to a physical computer with a different processor version. This needs to be done because Proliant DL320 and Proliant DL110 have different processor versions. This can be enabled from the virtual machine setting under processor configuration tab as shown in Figure 31.

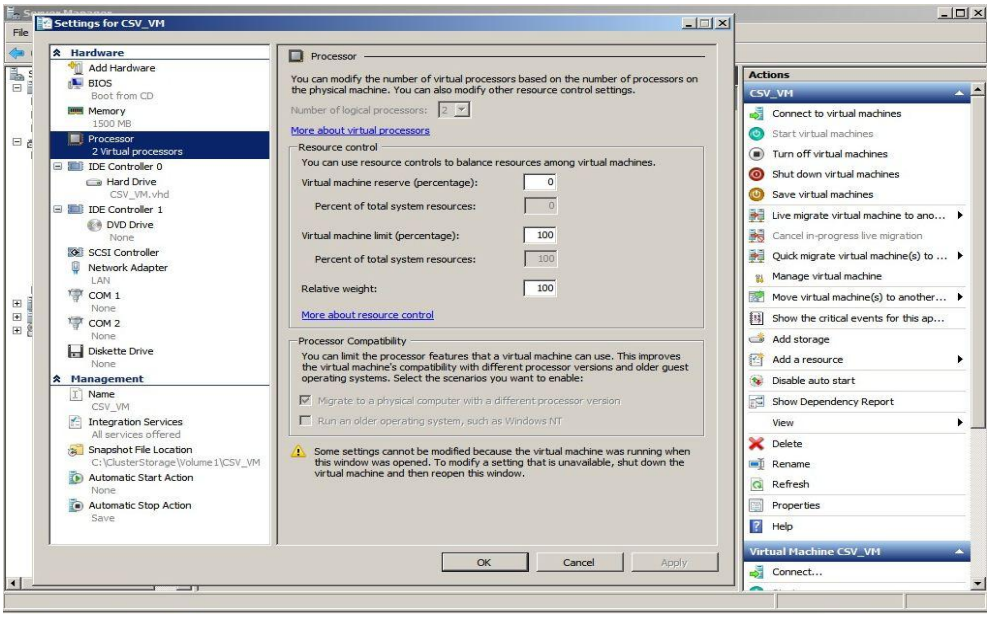

Figure 31 Virtual Machine Processor Configurations

The both storage systems were tested in this study so there was a need to install another virtual machine to use the host-based storage configurations. This was done with similar configurations as with the virtual machine named CSV_VM but the storage was configured to use iSCSI physical disk with specified drive letter on the host node. The virtual machine configuration file and virtual machines virtual hard drive are located on that drive. These both are showed in Figures 32 and 33.

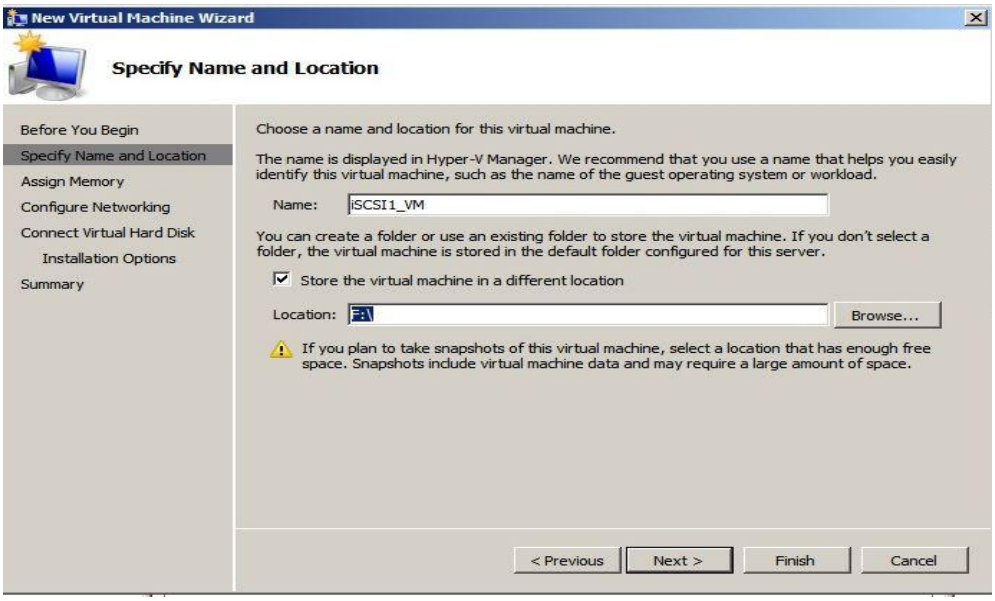

Figure 32 Second Virtual Machine Location and Name Configuration

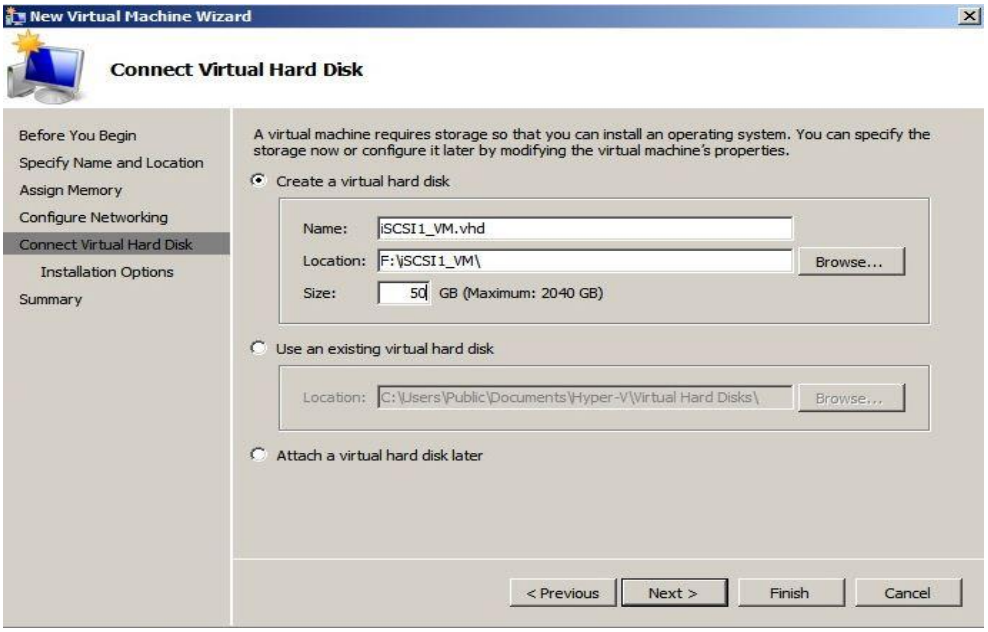

Figure 33 Second Virtual Machine Hard Disk Configurations

When the operating system was installed to another node named as iSCSI1_VM the environment was ready to be experimented. The experiments need to have Internet Information Services (IIS) sites to be configured on both virtual machines. And also the firewall must be disabled on the virtual machines so the virtual machines can response for ping command from the client.

The Internet Information Services is a Windows Server 2008 R2 role that provides web site services to the clients. The IIS was installed and from the configuration console of the IIS the basic File Transfer Protocol site was made and one folder was determined to the FTP site. Experiments in this study copied picture objects of random size with the FTP protocol to the virtual machine. Also the default web site was used to determine if the IIS service was again available after failovers has occurred. The next section deals with the experiments and gives the description of the purpose of the specific experiment.

4 TESTING FAILOVER CLUSTER

This section is to give experiment information of the study. The Hyper-V virtual machine high availability was tested in 5 different ways and both styles of the cluster storages were used in these tests. This section presents both the controlled and unexpected failures. Controlled failures include the live migration and quick migration of the failover cluster these are used when the maintenance is provided to the nodes. Unexpected failures concentrate on failures of the service or hardware. The tested unexpected failures are cluster service failure, node server power failure, network adapter failures, switch failure and storage hard drive failure.

4.1 Controlled Failures of Failover Cluster

Controlled failures illustrate a different ways to move virtual machines and iSCSI LUNs to another node in the cluster so that maintenance operations can be done on nodes without interrupting service to the clients.

Controlled failures are tested so that there will be an IIS site online which can be accessed. Files are copied from the client machine to the FTP site of the virtual machine. The virtual machine is pinged from the client side and timeout of the packets when they do not go through is measured with stopwatch.

Live migration is a new feature in the Windows Server 2008 R2 Failover Cluster service. Live migration will transfer a virtual machine from one node to another one inside the same cluster. Live Migration moves a virtual machine transparently to another node so that the connection to the virtual machine is available all the time and the virtual machine will not go offline. Live

migration can be done in the failover cluster manager. It is an action that can be performed to the virtual machine which is online.

The second controlled failure is to quick migrate the virtual machine from one node to another one within the cluster. Migration is done to compare the offline time difference between virtual machines that are configured to use cluster shared volume and host-based storage. Quick migration saves the virtual machine state and transfers it to another node where the virtual machine is restored from the saved state. Quick migration will make the virtual machine unreachable to the clients and the time of this unreachability is measured.

4.2 Unexpected Failures of Failover Cluster

Failover Cluster is built to improve the reliability of the server and at the same time improve availability of the services. There can be various failures on the hardware components of the server. Failure to most of these components will lead the server to shutdown unexpectedly. This unexpected shutdown is described with the lost power connection in this study. That was done by pulling the power cord from the power supply connector to have an unexpected shutdown to occur.

The intention of the second failure is to illustrate the failure of the clustering service. This actually describes that one Windows Server 2008 R2 operation system will not respond to the server so it will describe the node to have any software related failures. The test was made by selecting the node that is part of the cluster and the cluster service of the node is stopped.

The objective of the third failure is to illustrate the failure of the network adapters and their effect to the virtual machine when the local area network and iSCSI network adapter will fail. This also describes a failure of one cable that connects the storage or client to the cluster environment. This test was made so that network cable was pulled from the node where the virtual machine is running at the moment.

The meaning of the fourth unexpected failure is to pretend a failure of the switch. The test was made so that the power was plugged off one of the two switches. Another switch was operational all the time. Both switches cannot

go offline at the same time or the cluster and virtual machines will not be operational anymore.

The aim of the fifth unexpected failure is to demonstrate failure of the storage hard drive. One of the two hard drives was pulled out of the storage unit. This is the only way to test a storage that has only one power supply and one hard drive controller. If the power will go off or the controller fails the virtual machines and cluster service will go offline.

5 RESULTS AND ANALYSIS

This section deals with the results got from the experiments. The results are more considered in the discussion and conclusion section. All tests were made three times and the results displayed in this section are the average of these three measurements.

5.1 Controlled Failures of Failover Cluster

All storages and cluster components were configured so that the ownership of the components and storages is primarily owned by node1 and when the failures occur the needed ownership of the components were changed to other node named as node2.

Table 3 includes the results of the handled features. The table has four columns where the first column shows the failure type and the tested virtual machine. When a failure has a CSV marking it means that the test was made with the virtual machine that was using cluster shared volume storage. If the failure does not have the CSV marking it means that the test was made to the virtual machine that used host-based storage. Ping timeout column gives the time that virtual machine was not responding to the ping command. That column also tells the total migration time. The third column from the left indicates whether the file transfer was completed even if the failure occurred or not. The fourth column indicates if the configured service, in this study the Internet Information Services, was available after the failure occurred.

Table 3 Results of the Controlled Failures

Failure	**Ping timeout**	**Successful file transfer**	**Web site available before and after the failure**
Live Migration (CSV)	13 s (total migration time 5 min 26 s)	Yes	Yes
Live Migration	10 s (total migration time 4 min 50 s)	Yes	Yes
Quick Migration (CSV)	5 min 40 s (total migration time 5 min 47 s)	No	Yes
Quick Migration	45 s (total migration time 50s)	Yes	Yes

As shown above the handled failures will provide the service almost continuously to the clients even when the virtual machines are changing from one node to another inside the cluster. The Live migration took the virtual machine unavailable for 10-13 seconds and all services continued after the migration was completed. The quick migration gave an unexpected result when comparing the cluster shared volume to the host-based storage. The regular storage was migrated much faster than the cluster shared volume and it did continue the services immediately after the migration was done. The cluster shared volume took more time to migrate the virtual machine and it also failed to provide the services continuously. The explanation for this is that the cluster shared volume feature was provided with Windows Server 2008 R2 and therefore it is a new feature and will be updated in time. If the nodes had the latest updates installed this quick migration with the cluster shared volume should have gone faster.

5.2 Unexpected Failures of Failover Cluster

Unexpected failures are shown in Table 4. The table has the same columns as Table 3 but the failure types are different. The failure types have the

same marking principle with the cluster shared volume and host-based storages as in Table 3.

Table 4 Results of the Unexpected Failures

Failure	**Ping timeout**	**Successful file transfer**	**Web site available before and after the failure**
Service Failure (CSV)	2 min 25 s	No	Yes
Service Failure	1 min 10 s	No	Yes
Power failure (CSV)	2 min 23 s	No	Yes
Power failure	2 min 23 s	No	Yes
LAN (CSV)	NA	No (depents failure timeout)	Yes
LAN	NA	No (depents failure timeout)	Yes
iSCSI (CSV)	0s	Yes	Yes
iSCSI	0s	Yes	Yes
Switch (CSV)	0s	Yes	Yes
Switch	0s	Yes	Yes
Hard drive (CSV)	0s	Yes	Yes
Hard drive	0s	Yes	Yes

As seen in the unexpected failure results in Table 4 the virtual machine will go unavailable for about two minutes when a service or power failure occurs. This two minute unavailability is a result of an unexpected shutdown of the virtual machine. When the power will unexpectedly be out on the node server where the virtual machine is running it will shut down the connection to

the storage for a couple seconds. This leads the virtual machine to shut down because there is no Hyper-V host server to control the virtual machine. When the cluster notices the node failure it will automatically change the storage and virtual machine ownership to another node. This timeout can be shortened if the availability of the boot loading menu of the virtual machine is reduced from 30 seconds to less. The boot loading menu screen will be available for 30 seconds if virtual machine is unexpectedly shutdown.

When a local area network adapter failure occurred the clients could not connect to the virtual machine until the failure was fixed or the virtual machine was moved to another node. The single network connection to the local area network could not automatically change the virtual machine to another node because a heartbeat signal was still given from the iSCSI network.

The experiments of iSCSI and switch failures did not have any effect to the cluster because the iSCSI network was mirrored with two objects. If one switch failed, communications was continued through the other switch. And if iSCSI network adapter failed another one could still operate and keep the node connection online to the storage.

Hard drive failures of the QNAP did not have any effect to the service providing either. The hard drives use RAID level 1 where two hard drives have similar data on them and they are mirrored with each other. One hard drive failed and when it was plugged back the QNAP automatically started to rebuild the RAID and operation was available all time.

6 DISCUSSION AND CONCLUSIONS

As the results of the present study indicate, the Microsoft failover cluster is easy to build and manage. The planning should be done accurately because there are many objects that can be single points of failure if the configurations are not thought through.

In these experiments there were a few properties that could give slightly inaccurate result to the suggested configuration of the failover cluster. Firstly, the iSCSI network was configured to use only 100 MB connection because the switches used in this study could not support 1 GB connection speed. When the 1 GB connection is used it is suggested to use a jumbo frame fea-

ture on the network communication. Secondly, the file transfer was running when the migration operations were made and this slowed down the total migration time because the migration channel (LAN and iSCSI network) was also in use all the time for transfer purposes.

The results show that it is possible to build a clustered virtual machine environment with low cost equipment. The reliability can be improved when the Uninterruptible Power Supply (UPS) component is added to the environment to prevent unexpected shutdowns of the node servers. Also, all components should be mirrored. In this case that means local area network adapters and storage device. QNAP storage does not support real-time replication of the LUN disks so the storage should be considered again. In this study the QNAP storage was a single point of failure and if the data on it corrupts or the storage itself fails the clustered services are unavailable for the time of backup restoration or configuration of the new storage server and backup restoration. The Results indicated that the clustered virtual machine was unavailable for 2 minutes and 30 seconds at the maximum time with an unexpected failure. This is a rather good result considering the environment without failover cluster feature configured. Time that a virtual machine can be unavailable without failover cluster feature is tens, thousands or even tens of thousands times more than 2 minutes and 30 seconds. Without failover clustering the unavailability needs to be noticed by a person or a machine, and then someone needs to locate the failure and fix it. The time this could take varies but according to the experience of Datapalvelut.net the time to fix these could be hours or even days.

This study could have been done also with the different virtualization platforms and the results should be compared to the results gotten from this study. Microsoft is a rather new virtualization platform provider and this can make the results differ when different provider is used.

Failover Cluster feature gives more reliable service providing to the clients but it does not provide 100% availability. The servers are more automated and services will go offline for a couple minutes when an unexpected failure takes place. This is one aspect that needs to be considered. Are there any benefits to the company if their services are high available? As indicated by the results the servers will shut down when an unexpected failure happens and this might corrupt the installation of the Windows, hard drive partition or

database etc. Even with the failover cluster the backup is in an important role on the servers. The benefits of the failover cluster is to have the service to be available within 5 minutes if a hardware failure occurs and to have the server at a high available state when the maintenance is being carried. The costs of the offline time must be calculated and compared to the server hardware and software costs with and without a failover cluster.

REFERENCES

[1] Beowulf Cluster community, *Article written by Phil Merkey, assistant professor in mathematics and computer science at Michigan Technology University.* [WWW document] http://www.beowulf.org/overview/history.html (Accessed July 18, 2010)

[2] Sterling T. (2002) *Beowulf Cluster Computing With Linux*, United States of America: Massachusetts Institute of Technology.

[3] Baker M. (2000) *Cluster Computing White Paper,* University of Portsmouth, UK [WWW document] http://arxiv.org/ftp/cs/papers/0004/0004014.pdf (Accessed, June 01, 2010)

[4] Sportack M., Mohler J. (1997), *Windows NT Clustering Blueprints, 1st edition,* Macmillan Publishing CO., Indiapolis, USA.

[5] Microsoft, *Maximum number of nodes supported,* [WWW document] http://support.microsoft.com/kb/288778 (Accessed May 24, 2010)

[6] Microsoft, *Microsoft Windows NT Server Help: Cluster Server.* [WWW document] http://www.microsoft.com/resources/documentation/windowsnt/4/server/proddocs/en-us/clustsvr/mscsadm0.mspx?mfr=true (Accessed June 20, 2010)

[7] Microsoft, *What's New in Failover Clusters.* [WWW document] http://technet.microsoft.com/fi-fi/library/dd443539(en-us,WS.10).aspx (Accessed July 21, 2010)

[8] Microsoft, *Windows Server 2008 Failover Clustering Architecture Overview*. [WWW document] http://download.microsoft.com/download/3/b/5/3b51a025-7522-4686-aa16-8ae2e536034d/Windows%20Server%202008%20Failover%20Clustering%20Architecture%20Overview.doc (Accessed August 9, 2010)

[9] Microsoft, *Cluster Shared Volumes Support for Hyper-V.* [WWW Document] http://technet.microsoft.com/en-us/library/dd630633(WS.10).aspx (Accessed October 15, 2010)

[10] Hewlett-Packard, *HP Proliant DL320 G6 Server data sheet.* [WWW document] http://h18004.www1.hp.com/products/quickspecs/DS_00188/DS_00188.pdf (Accessed March 1, 2010)

[11] Hewlett-Packard, HP Proliant DL110 G4 Server Series. [WWW document] http://h10010.www1.hp.com/wwpc/in/en/sm/WF10a/15351-15351-241434-3328424-3328424-3186395.html (Accessed March 1, 2010)