



## Cisco Virtualization Solution for EMC VSPEX with Microsoft Windows Server 2012 Hyper-V for 50 Vir- tual Machines

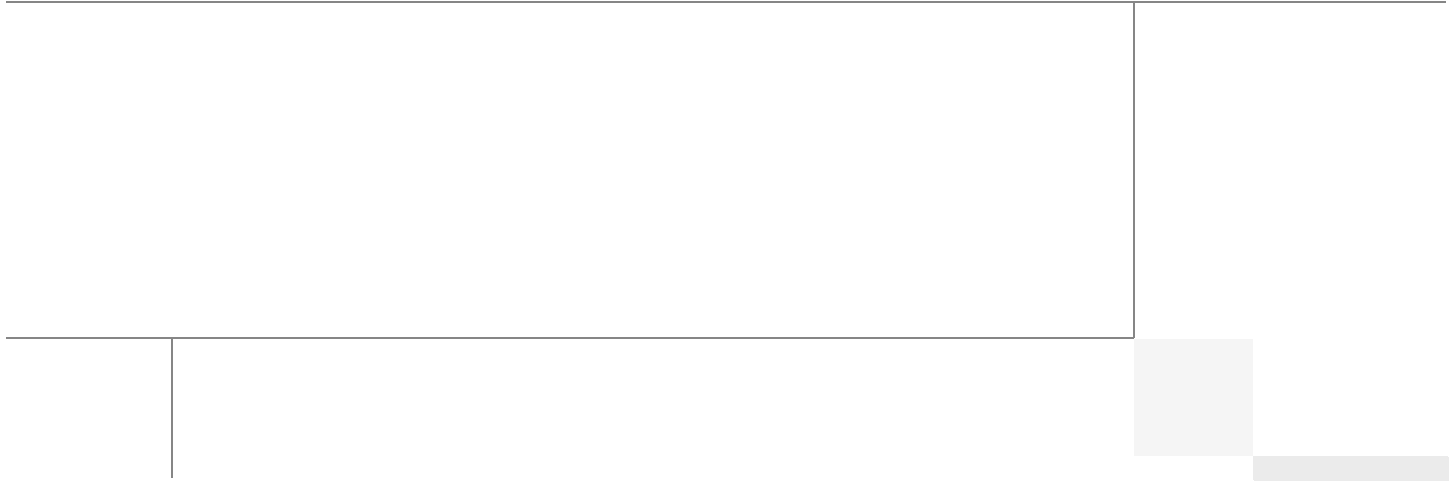
Last Updated: May 30, 2013



Cisco  
Validated  
Design



Building Architectures to Solve Business Problems



## About the Authors



Sanjeev Naldurgkar

### **Sanjeev Naldurgkar, Technical Marketing Engineer, Server Access Virtualization Business Unit, Cisco Systems**

Sanjeev Naldurgkar is a Technical Marketing Engineer at Cisco Systems with Server Access Virtualization Business Unit (SAVBU). With over 12 years of experience in information technology, his focus areas include UCS, Microsoft product technologies, server virtualization, and storage technologies. Prior to joining Cisco, Sanjeev was Support Engineer at Microsoft Global Technical Support Center. Sanjeev holds a Bachelor's Degree in Electronics and Communication Engineering and Industry certifications from Microsoft, and VMware.

# Acknowledgements

For their support and contribution to the design, validation, and creation of the Cisco Validated Design, I would like to thank:

- Tim Cerling-Cisco
- Vadiraja Bhatt-Cisco
- Vijaykumar D-Cisco
- Bathu Krishnan-Cisco
- Sindhu Sudhir-Cisco
- Kevin Phillips-EMC
- John Moran-EMC
- Kathy Sharp-EMC



# About Cisco Validated Design (CVD) Program

---

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit:

<http://www.cisco.com/go/designzone>

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at <http://www.cisco.com/go/trademarks>. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.



# Cisco Virtualization Solution for EMC VSPEX with Microsoft Windows Server 2012 Hyper-V for 50 Virtual Machines

---

## Executive Summary

Cisco solution for EMC VSPEX proven and modular infrastructures are built with best of-breed technologies to create complete virtualization solutions that enable you to make an informed decision in the hypervisor, compute, and networking layers. VSPEX eases server virtualization planning and configuration burdens. VSPEX accelerate your IT Transformation by enabling faster deployments, greater flexibility of choice, efficiency, and lower risk. This Cisco Validated Design document focuses on the Microsoft Hyper-V architecture for 50 virtual machines with Cisco solution for EMC VSPEX.

## Introduction

As part of an effort to improve and enhance the performance and capabilities of its product line, Cisco and EMC from time to time release revisions of its hardware and software. Therefore, some functions described in this guide may not be supported by all revisions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

## Target Audience

The reader of this document is expected to have the necessary training and background to install and configure Microsoft Hyper-V, EMC VNXe, and Cisco Nexus 3048 switches, and Cisco Unified Computing System (UCS) C220 M3 rack servers. External references are provided where applicable and it is recommended that the reader be familiar with these documents.

Readers are also expected to be familiar with the infrastructure and database security policies of the customer installation.



---

**Corporate Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

Copyright 2013 Cisco Systems, Inc. All rights reserved.

## Purpose of this Document

This document describes the steps required to deploy and configure a Cisco solution for EMC VSPEX for Microsoft Hyper-V architectures to a level that will allow for confirmation that the basic components and connections are working correctly. The document covers one Microsoft Hyper-V architecture i.e. Hyper-V for 50 Virtual Machines. While readers of this document are expected to have sufficient knowledge to install and configure the products used, configuration details that are important to this solution's performance are specifically mentioned.

## Business Needs

VSPEX solutions are built with proven best-of-breed technologies to create complete virtualization solutions that enable you to make an informed decision in the hypervisor, server, and networking layers coupled with EMC unified Storage and Next Generation Backup. VSPEX infrastructures accelerate your IT transformation by enabling faster deployments, greater flexibility of choice, efficiency, and lower risk.

Business applications are moving into the consolidated compute, network, and storage environment. Cisco solution for EMC VSPEX for Microsoft Hyper-V helps to reduce every component of a traditional deployment. The complexity of integration management is reduced while maintaining the application design and implementation options. Administration is unified, while process separation can be adequately controlled and monitored. The following are the business needs for the Cisco solution of EMC VSPEX Microsoft Hyper-V architectures:

- Provide an end-to-end virtualization solution to take full advantage of unified infrastructure components.
- Provide a Cisco VSPEX for Microsoft Hyper-V Infrastructure as a Service (IaaS) solution for efficiently virtualizing up to 50 virtual machines for varied customer use cases.
- Provide a reliable, flexible, and scalable reference design

## Solutions Overview

### Cisco Solution for EMC VSPEX Microsoft Hyper-V Architectures

This solution provides an end-to-end architecture with Cisco, EMC, and Microsoft technologies that demonstrate support for up to 50 generic virtual machines and provides high availability and server redundancy.

The following are the components used for the design and deployment:

- Cisco C-series Unified Computing System servers
- Cisco Nexus 3000 series switches
- Cisco virtual Port-Channels for network load balancing and high availability
- EMC VNXe3150
- EMC Amavar
- Microsoft Windows Server 2012 Hyper-V

The solution is designed to host scalable, mixed application workloads. The scope of this CVD is limited to the Cisco solution for EMC VSPEX Microsoft Hyper-V solutions for 50 virtual machines only. For additional scale and different virtualization solution, please refer to other VSPEX architectures.

## Technology Overview

### Cisco Unified Computing System

The Cisco Unified Computing System is a next-generation data center platform that unites computing, network, storage access, and virtualization into a single cohesive system.

The main components of the Cisco UCS are:

- **Computing**—The system is based on an entirely new class of computing system that incorporates rack mount and blade servers based on Intel Xeon E-2600 Series Processors. The Cisco UCS servers offer the patented Cisco Extended Memory Technology to support applications with large datasets and allow more virtual machines per server.
- **Network**—The system is integrated onto a low-latency, lossless, 10-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing networks which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables, and by decreasing the power and cooling requirements.
- **Virtualization**—The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- **Storage access**—The system provides consolidated access to both SAN storage and Network Attached Storage (NAS) over the unified fabric. By unifying the storage access the Cisco Unified Computing System can access storage over Ethernet, Fibre Channel, Fibre Channel over Ethernet (FCoE), and iSCSI. This provides customers with choice for storage access and investment protection. In addition, the server administrators can pre-assign storage-access policies for system connectivity to storage resources, simplifying storage connectivity, and management for increased productivity.

The Cisco Unified Computing System is designed to deliver:

- A reduced Total Cost of Ownership (TCO) and increased business agility.
- Increased IT staff productivity through just-in-time provisioning and mobility support.
- A cohesive, integrated system which unifies the technology in the data center.
- Industry standards supported by a partner ecosystem of industry leaders.

### Cisco UCS C220 M3 Rack-Mount Servers

Building on the success of the Cisco UCS C200 M2 Rack Servers, the enterprise-class Cisco UCS C220 M3 server further extends the capabilities of the Cisco Unified Computing System portfolio in a 1-rack-unit (1RU) form factor. And with the addition of the Intel® Xeon® processor E5-2600 product family, it delivers significant performance and efficiency gains.

**Figure 1** *Cisco UCS C220 M3 Rack Server*



The Cisco UCS C220 M3 offers up to 256 GB of RAM, up to eight drives or SSDs, and two 1GE LAN interfaces built into the motherboard, delivering outstanding levels of density and performance in a compact package.

## Cisco Nexus 3048 Switch

The Cisco Nexus® 3048 Switch is a line-rate Gigabit Ethernet top-of-rack (ToR) switch and is part of the Cisco Nexus 3000 Series Switches portfolio. The Cisco Nexus 3048, with its compact one-rack-unit (1RU) form factor and integrated Layer 2 and 3 switching, complements the existing Cisco Nexus family of switches. This switch runs the industry-leading Cisco® NX-OS Software operating system, providing customers with robust features and functions that are deployed in thousands of data centers worldwide.

**Figure 2** *Cisco Nexus 3048 Switch*



## EMC Storage Technologies and Benefits

The EMC VNXe™ family is optimized for virtual applications delivering industry-leading innovation and enterprise capabilities for file, block, and object storage in a scalable, easy-to-use solution. This next-generation storage platform combines powerful and flexible hardware with advanced efficiency, management, and protection software to meet the demanding needs of today's enterprises.

The VNXe™ series is powered by Intel Xeon processor, for intelligent storage that automatically and efficiently scales in performance, while ensuring data integrity and security.

The VNXe series is purpose-built for the IT manager in smaller environments and the VNX series is designed to meet the high-performance, high-scalability requirements of midsize and large enterprises. The EMC VNXe and VNX storage arrays are multi-protocol platform that can support the iSCSI, NFS, and CIFS protocols depending on the customer's specific needs. The solution was validated using iSCSI for data storage.

VNXe series storage arrays have following customer benefits:

- Next-generation unified storage, optimized for virtualized applications
- Capacity optimization features including compression, deduplication, thin provisioning, and application-centric copies
- High availability, designed to deliver five 9s availability
- Multiprotocol support for file and block
- Simplified management with EMC Unisphere™ for a single management interface for all network-attached storage (NAS), storage area network (SAN), and replication needs

## Software Suites Available

- Remote Protection Suite — Protects data against localized failures, outages, and disasters.
- Application Protection Suite — Automates application copies and proves compliance.
- Security and Compliance Suite — Keeps data safe from changes, deletions, and malicious activity.

## Software Packs Available

Total Value Pack — Includes all protection software suites and the Security and Compliance Suite

This is the available EMC protection software pack.

The VNXe™ series is powered by Intel Xeon processor, for intelligent storage that automatically and efficiently scales in performance, while ensuring data integrity and security.

The VNXe series is purpose-built for the IT manager in smaller environments. The EMC VNXe storage arrays are multi-protocol platforms that can support the iSCSI, NFS, and CIFS protocols depending on the customer's specific needs. The solution was validated using iSCSI for data storage.

## EMC Avamar

EMC's Avamar® data deduplication technology seamlessly integrates into virtual environments, providing rapid backup and restoration capabilities. Avamar's deduplication results in vastly less data traversing the network, and greatly reduces the amount of data being backed up and stored – translating into storage, bandwidth and operational savings.

The following are two of the most common recovery requests made to backup administrators:

**File-level recovery**—Object-level recoveries account for the vast majority of user support requests. Common actions requiring file-level recovery are—individual users deleting files, applications requiring recoveries, and batch process-related erasures.

**System recovery**—Although complete system recovery requests are less frequent in number than those for file-level recovery, this bare metal restore capability is vital to the enterprise. Some common root causes for full system recovery requests are—viral infestation, registry corruption, or unidentifiable unrecoverable issues.

The Avamar System State protection functionality adds backup and recovery capabilities in both of these scenarios.

## Microsoft Windows Server 2012

Hyper-V is an integral part of Windows Server and provides a foundational virtualization platform that enables you to transition to the cloud. With Windows Server 2012 you get a compelling solution for core virtualization scenarios – production server consolidation, dynamic datacenter, business continuity, VDI, and test & development.

Hyper-V provides you better flexibility with features like live migration and cluster shared volumes for storage flexibility.

Hyper-V also delivers greater scalability with support for up to 320 logical processors on hardware, 4 TB of physical memory, 64 virtual processors, and up to 1 TB of memory on a virtual machine. Up to 64 nodes and 8,000 virtual machines in a cluster also can be supported. With Non-Uniform Memory Access (NUMA) support inside virtual machines, guest operating systems and applications can make

intelligent NUMA decisions and improvements to the dynamic memory feature of Hyper-V in Windows Server 2012; you can attain higher consolidation numbers with improved reliability for restart operations.

## Architectural overview

This CVD focuses on Microsoft Hyper-V solution for up to 50 virtual machines.

For the VSPEX solution, the reference workload was defined as a single virtual machine. Characteristics of a virtual machine are defined in [Table 1](#).

**Table 1** *Virtual Machine Characteristics*

Characteristics	Value
Virtual machine operating system	Microsoft Windows Server 2012
Virtual processor per virtual machine (vCPU)	1
RAM per virtual machine	2 GB
Available storage capacity per virtual machine	100 GB
I/O operations per second (IOPS) per VM	25
I/O pattern	Random
I/O read/write ratio	2:1

See “[Sizing Guideline](#)” section on [page 15](#) for more detailed information.

## Solution architecture overview

[Table 2](#) lists the mix of hardware components, their quantities and software components used for Microsoft Hyper-V solution for 50 Virtual Machines.

**Table 2** *Hardware and Software Components*

Components	Microsoft Hyper-V 50 VMs
Servers	3 Cisco C220 M3 Rack-Mount Servers
Adapters	2 Cisco 1G Ethernet I350 LOM 1 Broadcom NetXtreme II 5709 quad-port per server
Network Switches	2 Cisco Nexus 3048 switches
Storage	EMC VNXe3150
Network Speed	1G Ethernet
Hypervisor	Microsoft Windows Server 2012 Hyper-V

[Table 3](#) lists the various hardware and software versions of the components which occupies different tiers of the Cisco solution for EMC VSPEX Microsoft architectures under test.

**Table 3** *Firmware and Software Versions of Components*

Vendor	Name	Version
Cisco	C220 M3 Servers	1.4(7a) – CIMC
		C220M3.1.4.7b.0 - BIOS
Cisco	Nexus 3048 Switches	5.0(3)U2(2b)
EMC	VNXe3150	2.4.0.20932
EMC	Amavar	6.1 SP1
EMC	Data Domain OS	5.3
Micorsoft	Windows Server	2012 Datacenter

Table 4 outlines the C220 M3 server configuration across all the Microsoft Hyper-V architectures. The table shows the configuration on per server basis.

**Table 4** *Cisco UCS C220 M3 Server Hardware Configuration*

Components	Capacity
Memory (RAM)	64 GB (8x8MB DIMM)
Processor	2 x Intel® Xeon ® E5-2650 CPUs, 2 GHz, 8 cores, 16 threads
Network Adapter	2 x Cisco 1GigE I350 LOM (Lan-on-motherboard)
Local Storage	Cisco UCS RAID SAS 2008M-8i Mezzanine Card, With 2 x 67 GB slots for RAID 1 configuration each

## Storage Guidelines

The architecture diagram in this section shows the physical disk layout. Disk provisioning on the VNXe series is simplified through the use of wizards, so that administrators do not choose which disks belong to a given storage pool. The wizard may choose any available disk of the proper type, regardless of where the disk physically resides in the array

The reference architecture uses the following configuration:

Following are the disk allocations for VSPEX M50 architectures:

- For 50 VMs, Forty-five 600 GB SAS disks are allocated to a single storage pool as nine 4+1 RAID 5 groups (sold as 5-disk packs).
- EMC recommends that in addition to the above numbers at least one hot spare disk is allocated for each 30 disks of a given type.

The VNX/VNXe family is designed for five 9s availability by using redundant components throughout the array. All of the array components are capable of continued operation in case of hardware failure. The RAID disk configuration on the array provides protection against data loss due to individual disk failures, and the available hot spare drives can be dynamically allocated to replace a failing disk.



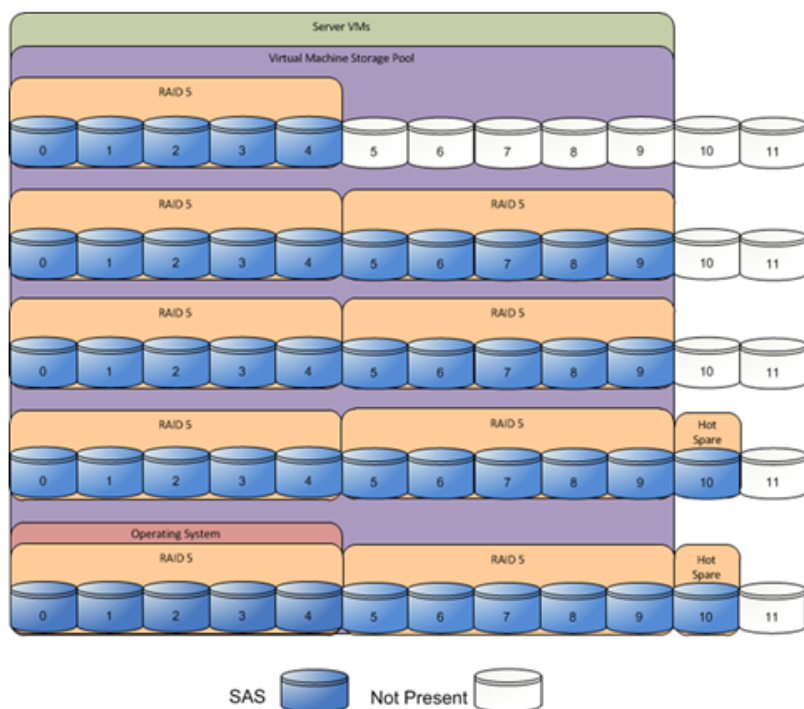
**Figure 3 Target Storage layout for EMC VSPEX M50 Solution**

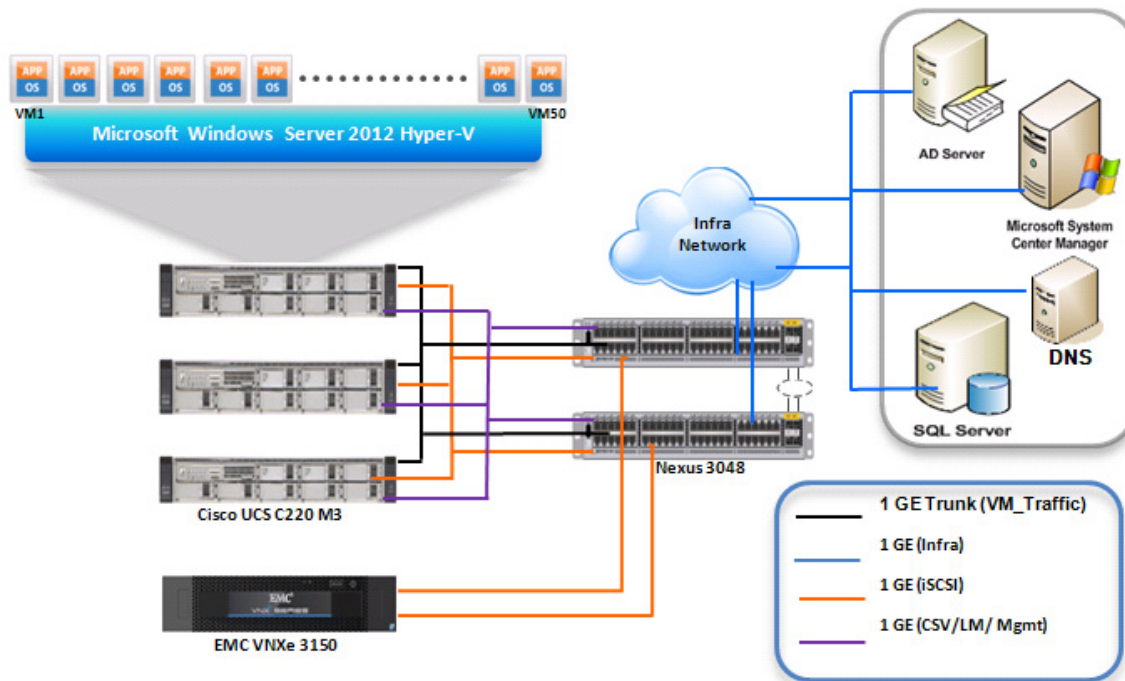
Table 5 provides size of datastores for M50 architecture laid out in Figure 3.

**Table 5 Datastore Details for M50 Architecture**

Parameters	50 Virtual Machines
Disk capacity and type	300GB SAS
Number of disks	45
RAID type	4 + 1 RAID 5 groups
Number of RAID groups	9

The VSPEX M50 reference architecture assumes there is an existing infrastructure / management network available where a virtual machine or physical machine hosting SCVMM server, Database server and Windows Active Directory and DNS servers are present. Figure 4 demonstrate high level solution architecture for up to 50 virtual machines.

**Figure 4** *Reference Architecture for 50 Virtual Machines*



As it is evident in the above diagrams, following are the high level design points of Microsoft Hyper-V architectures:

- Only Ethernet is used as network layer 2 media to access storage as well as TCP/IP network
- Infrastructure network is on a separate 1GE uplink network
- Network redundancy is built in by providing two switches, two storage controllers and redundant connectivity for data, storage, and infrastructure networking.

This design does not dictate or require any specific layout of infrastructure network which hosts the SCVMM, Database, and Active Directory servers. However, design does require accessibility of certain VLANs from the infrastructure network to reach the servers.

Microsoft Windows Server 2012 Hyper-V is used as hypervisor operating system on each server and is installed on local hard drives. Typical maximum load is 25 virtual machines per server.

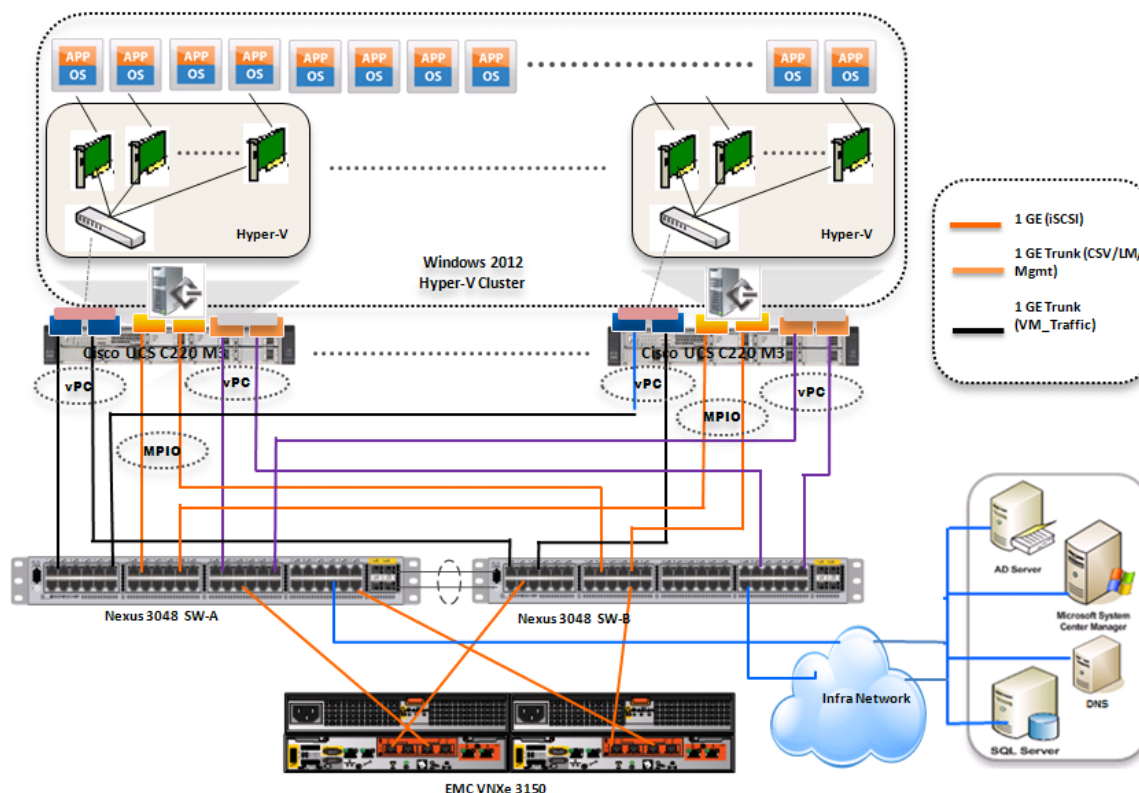
## Architecture for 50 Microsoft Hyper-V virtual machines

Figure 5 demonstrates logical layout of 50 Microsoft Hyper-V virtual machines. Following are the key aspects of this solution:

- Three Cisco C220 M3 servers are used.
- The solution uses two Nexus 3048 switches, dual-port Cisco 1GigE I350 LOM and quad-port Broadcom 1Gbps NIC. This results in the 1Gbps solution for the storage access.
- Virtual port-channels and NIC teaming of Ethernet adapters on the host side provide high-availability and load balancing.

- Microsoft Windows Server 2012 in-built NIC teaming of the adapters on the host provide load balancing and redundancy for data traffic as shown in Figure 5. Team 1 has two mLOM ports for VM traffic. Team 2 has two Broadcom ports for all cluster (Heartbeat, CSV and Live Migration) and host management traffic. In case NICs used for iSCSI, Microsoft Multipath Input/Output (MPIO) is used to provide improved performance and redundancy.
- EMC VNXe3150 is used as a storage array.

**Figure 5** Logical Layout Diagram for 50 Virtual Machines



## Sizing Guideline

In any discussion about virtual infrastructures, it is important to first define a reference workload. Not all servers perform the same tasks, and it is impractical to build a reference that takes into account every possible combination of workload characteristics.

## Defining the Reference Workload

To simplify the discussion, we have defined a representative reference workload. By comparing your actual usage to this reference workload, you can extrapolate which reference architecture to choose.

For the VSPEX solutions, the reference workload was defined as a single virtual machine. This virtual machine characteristics is shown in Table 1. This specification for a virtual machine is not intended to represent any specific application. Rather, it represents a single common point of reference to measure other virtual machines.

## Applying the Reference Workload

When considering an existing server that will move into a virtual infrastructure, you have the opportunity to gain efficiency by right-sizing the virtual hardware resources assigned to that system.

The reference architectures create a pool of resources sufficient to host a target number of reference virtual machines as described above. It is entirely possible that your virtual machines may not exactly match the specifications above. In that case, you can say that a single specific virtual machine is the equivalent of some number of reference virtual machines, and assume that that number of virtual machines have been used in the pool. You can continue to provision virtual machines from the pool of resources until it is exhausted. Consider these examples:

### **Example 1     Custom Built Application**

A small custom-built application server needs to move into this virtual infrastructure. The physical hardware supporting the application is not being fully utilized at present. A careful analysis of the existing application reveals that the application can use one processor and needs 3 GB of memory to run normally. The IO workload ranges between 4 IOPS at idle time to 15 IOPS when busy. The entire application is only using about 30 GB on local hard drive storage.

Based on these numbers, the following resources are needed from the resource pool:

- CPU resources for one VM
- Memory resources for two VMs
- Storage capacity for one VM
- IOPS for one VM

In this example, a single virtual machine uses the resources of two of the reference VMs. If the original pool had the capability to provide 50 VMs worth of resources, the new capability is 48 VMs.

### **Example 2     Point of Sale System**

The database server for a customer's point-of-sale system needs to move into this virtual infrastructure. It is currently running on a physical system with four CPUs and 16 GB of memory. It uses 200 GB storage and generates 200 IOPS during an average busy cycle.

The following are the requirements to virtualize this application:

- CPUs of four reference VMs
- Memory of eight reference VMs
- Storage of two reference VMs
- IOPS of eight reference VMs

In this case the one virtual machine uses the resources of eight reference virtual machines. If this was implemented on a resource pool for 50 virtual machines, there are 42 virtual machines of capability remaining in the pool.

### **Example 3     Web Server**

The customer's web server needs to move into this virtual infrastructure. It is currently running on a physical system with two CPUs and 8GB of memory. It uses 25 GB of storage and generates 50 IOPS during an average busy cycle.

The following are the requirements to virtualize this application:

- CPUs of two reference VMs
- Memory of four reference VMs
- Storage of one reference VMs
- IOPS of two reference VMs

In this case the virtual machine would use the resources of four reference virtual machines. If this was implemented on a resource pool for 50 virtual machines, there are 46 virtual machines of capability remaining in the pool.

### Summary of Example

The three examples presented illustrate the flexibility of the resource pool model. In all three cases the workloads simply reduce the number of available resources in the pool. If all three examples were implemented on the same virtual infrastructure, with an initial capacity of 50 virtual machines they can all be implemented, leaving the capacity of thirty six reference virtual machines in the resource pool.

In more advanced cases, there may be tradeoffs between memory and I/O or other relationships where increasing the amount of one resource decreases the need for another. In these cases, the interactions between resource allocations become highly complex, and are outside the scope of this document. However, once the change in resource balance has been examined, and the new level of requirements is known; these virtual machines can be added to the infrastructure using the method described in the examples. You can also use the Microsoft Assessment and Planning (MAP) Toolkit to assist in the analysis of the current workload. It can be downloaded from <http://www.microsoft.com/map>.

## Networking Configuration Guidelines

This document provides details for setting up a redundant, highly-available configuration. As such, references are made as to which component is being configured with each step whether that be A or B. For example, SP A and SP B, are used to identify the two EMC VNXe storage controllers that are provisioned with this document while Switch A and Switch B identify the pair of Cisco Nexus switches that are configured. Additionally, this document details steps for provisioning multiple UCS hosts and these are identified sequentially, M50N1 and M50N2, and so on. Finally, when indicating that the reader should include information pertinent to their environment in a given step, this is indicated with the inclusion of *<italicized/regular text>* as part of the command. See the following example for the VLAN create command on Nexus:

```
switchA(config)# vlan {vlan-id | vlan-range}
```

Example:

```
switchA(config)# vlan <storage VLAN ID>
```

This document is intended to allow the reader to fully configure the customer environment. In order to do so, there are various steps which will require you to insert your own naming conventions, IP addresses, and VLAN schemes, as well as record appropriate iSCSI IQN name or MAC addresses.

[Table 7](#) details the list of VLANs necessary for deployment as outlined in this guide

## VSPEX Configuration Guidelines

The configuration for Cisco solution for EMC VSPEX Microsoft Hyper-V architectures is divided into the following steps:

1. Pre-deployment tasks

2. Cabling Information
3. Prepare and Configure the Cisco Nexus Switches
4. Infrastructure Servers
5. Prepare the Cisco UCS C220 M3 Servers
6. Prepare the EMC VNXe Series Storage
7. Microsoft Windows Failover Cluster Setup
8. Test the installation

Next pages go into details of each section mentioned above.

## Pre-deployment Tasks

Pre-deployment tasks include procedures that do not directly relate to environment installation and configuration, but whose results will be needed at the time of installation. Examples of pre-deployment tasks are collection of hostnames, IP addresses, VLAN IDs, license keys, installation media, and so on. These tasks should be performed before the customer visit to decrease the time required onsite.

- Gather documents—Gather the related documents listed in the Preface. These are used throughout the text of this document to provide detail on setup procedures and deployment best practices for the various components of the solution.
- Gather tools—Gather the required and optional tools for the deployment. Use [Table 2](#), [Table 3](#) and [Table 4](#) to confirm that all equipment, software, and appropriate licenses are available before the deployment process.
- Gather data—Collect the customer-specific configuration data for networking, naming, and required accounts. Enter this information into the “[Customer Configuration Data Sheet](#)” section on page 124 for reference during the deployment process.

## Customer Configuration Data

To reduce the onsite time, information such as IP addresses and hostnames should be assembled as part of the planning process.

“[Customer Configuration Data Sheet](#)” section on page 124 provides a set of tables to maintain a record of relevant information. This form can be expanded or contracted as required, and information may be added, modified, and recorded as deployment progresses.

Additionally, complete the *VNXe Series Configuration Worksheet*, available on the EMC online support website, to provide the most comprehensive array-specific information.

## Infrastructure Servers

Most environments will already have DNS and Active Directory services in their infrastructure either running on a virtual machine or on a physical server. This section will not cover the installation and configuration of DNS and Active Directory Domain Controllers.

The following infrastructure servers were used to validate the VSPEX Microsoft Hyper-V architectures.

**Table 6**      **Infrastructure Server Details**

Server Name	Role	IP Address	OS
M50AD.M50VSPEX.COM	DC,DNS and DHCP	10.29.150.90-Mgmt 10.10.23.90-vm_traffic	Windows Server 2012

## VSPEX M50 Configuration Details

### Cabling Information

The following information is provided as a reference for cabling the physical equipment in a VSPEX M50 environment. [Figure 7](#) and [Figure 8](#) in this section provide both local and remote device and port locations in order to simplify cabling requirements.

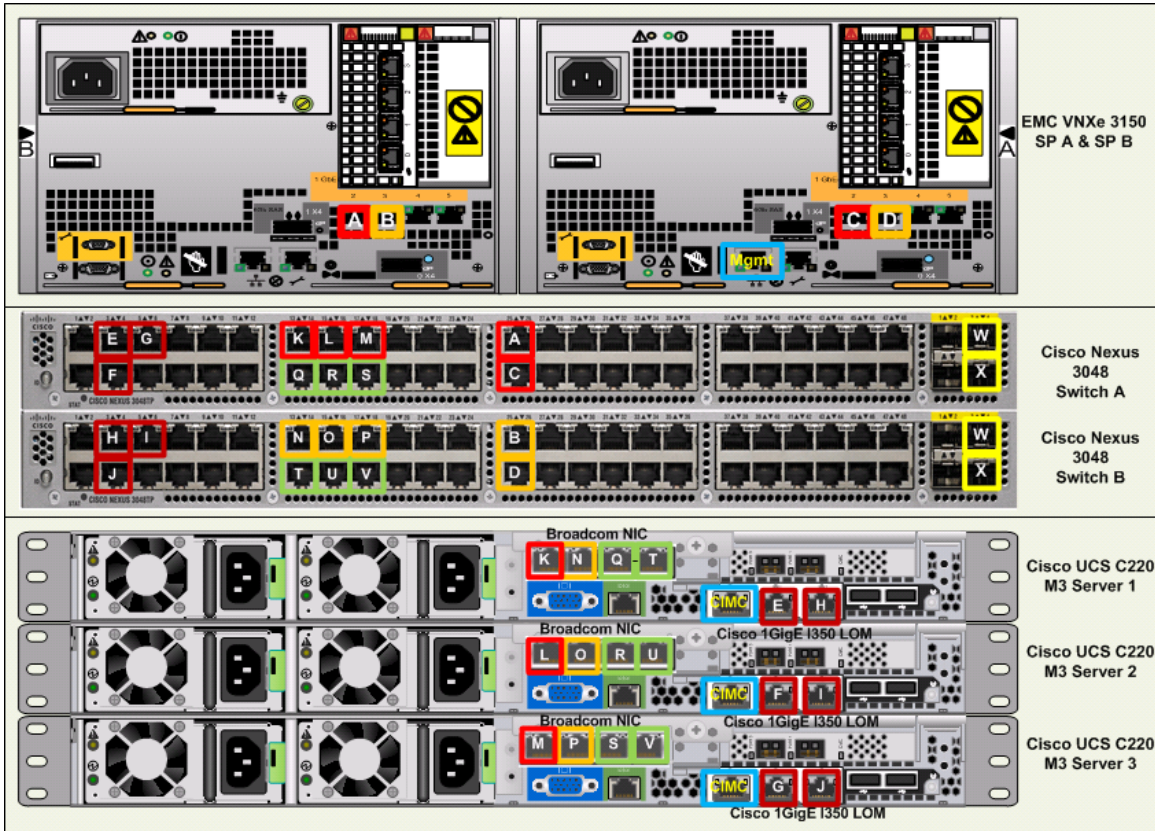
This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site.

Be sure to follow the cable directions in this section. Failure to do so will result in necessary changes to the deployment procedures that follow because specific port locations are mentioned. Before starting, be sure that the configuration matches what is described in [Figure 6](#), [Figure 7](#), and [Figure 8](#).

[Figure 6](#) shows a VSPEX M50 cabling diagram. The labels indicate connections to end points rather than port numbers on the physical device. For example, connection A is a 1 Gb target port connected from EMC VNxe3150 SP B to Cisco Nexus 3048 A and connection R is a 1 Gb target port connected from Broadcom NIC 3 on Server 2 to Cisco Nexus 3048 B. Connections W and X are 10 Gb vPC peer-links connected from Cisco Nexus 3048 A to Cisco Nexus 3048 B.



Figure 6 VSPEX M50 Cabling Diagram



From [Figure 7](#) and [Figure 8](#) in this section, there are five major cabling sections in these architectures:

1. Inter switch links
2. Data connectivity for servers (trunk links)
3. Management connectivity for servers
4. Storage connectivity
5. Infrastructure connectivity.



**Figure 7 Cisco Nexus 3048-A Ethernet Cabling Information**

Cable ID on both ends	Ethernet Interface	VLAN ID	Mode	Speed	Port Channel	Remote Device Port
E	Eth1/3	1, 23	trunk	1G	3	C220 Srv1- 1GE LOM 1
F	Eth1/4	1,23	trunk	1G	4	C220 Srv2- 1GE LOM 1
G	Eth1/5	1,23	trunk	1G	5	C220 Srv3- 1GE LOM 1
W	Eth1/51	1,20,22,23,24	trunk	10G	10	VPC peer link
X	Eth1/52	1,20,22,23,24	trunk	10G	10	VPC peer link
K	Eth1/13	20	access	1G	--	C220 Srv1- Broadcom NIC 1
L	Eth1/15	20	access	1G	--	C220 Srv2- Broadcom NIC 1
M	Eth1/17	20	access	1G	--	C220 Srv3- Broadcom NIC 1
Q	Eth1/14	1,22,24	trunk	1G	14	C220 Srv1- Broadcom NIC 3
R	Eth1/16	1,22,24	trunk	1G	16	C220 Srv2- Broadcom NIC 3
S	Eth1/18	1,22,24	trunk	1G	18	C220 Srv3- Broadcom NIC 3
Not shown	Eth1/9	1, 23	trunk	10G	15	Uplink to Infra n/w
Not shown	Eth1/10	1,23	trunk	10G	17	Uplink to Infra n/w
A	Eth1/25	20	access	1G	-	VNXe3150 (eth10) - SPA
C	Eth1/26	20	access	1G	-	VNXe3150 (eth10) - SPB

**Figure 8 Cisco Nexus 3048-B Ethernet Cabling Information**

Cable ID on both ends	Ethernet Interface	VLAN ID	Mode	Speed	Port Channel	Remote Device Port
H	Eth1/3	1, 23	trunk	1G	3	C220 Srv1- 1GE LOM 2
I	Eth1/4	1,23	trunk	1G	4	C220 Srv2- 1GE LOM 2
J	Eth1/5	1,23	trunk	1G	5	C220 Srv3- 1GE LOM 2
Y	Eth1/51	1,21,22,23,24	trunk	10G	10	VPC peer link
Z	Eth1/52	1,21,22,23,24	trunk	10G	10	VPC peer link
N	Eth1/13	21	access	1G	--	C220 Srv1- Broadcom NIC 2
O	Eth1/15	21	access	1G	--	C220 Srv2- Broadcom NIC 2
P	Eth1/17	21	access	1G	--	C220 Srv3- Broadcom NIC 2
T	Eth1/14	1,22,24	trunk	1G	14	C220 Srv1- Broadcom NIC 4
U	Eth1/16	1,22,24	trunk	1G	16	C220 Srv2- Broadcom NIC 4
V	Eth1/18	1,22,24	trunk	1G	18	C220 Srv3- Broadcom NIC 4
Not shown	Eth1/9	1,23	trunk	10G	15	Uplink to Infra n/w
Not shown	Eth1/10	1,23	trunk	10G	17	Uplink to Infra n/w
B	Eth1/25	21	access	1G	-	VNXe3150 (eth11) - SPA
D	Eth1/26	21	access	1G	-	VNXe3150 (eth11) - SPB

Connect all the cables as outlined in the [Figure 6](#), [Figure 7](#), and [Figure 8](#).

## Prepare and Configure the Cisco Nexus 3048 Switch

The following section provides a detailed procedure for configuring the Cisco Nexus 3048 switches for use in EMC VSPEX M50 solution.

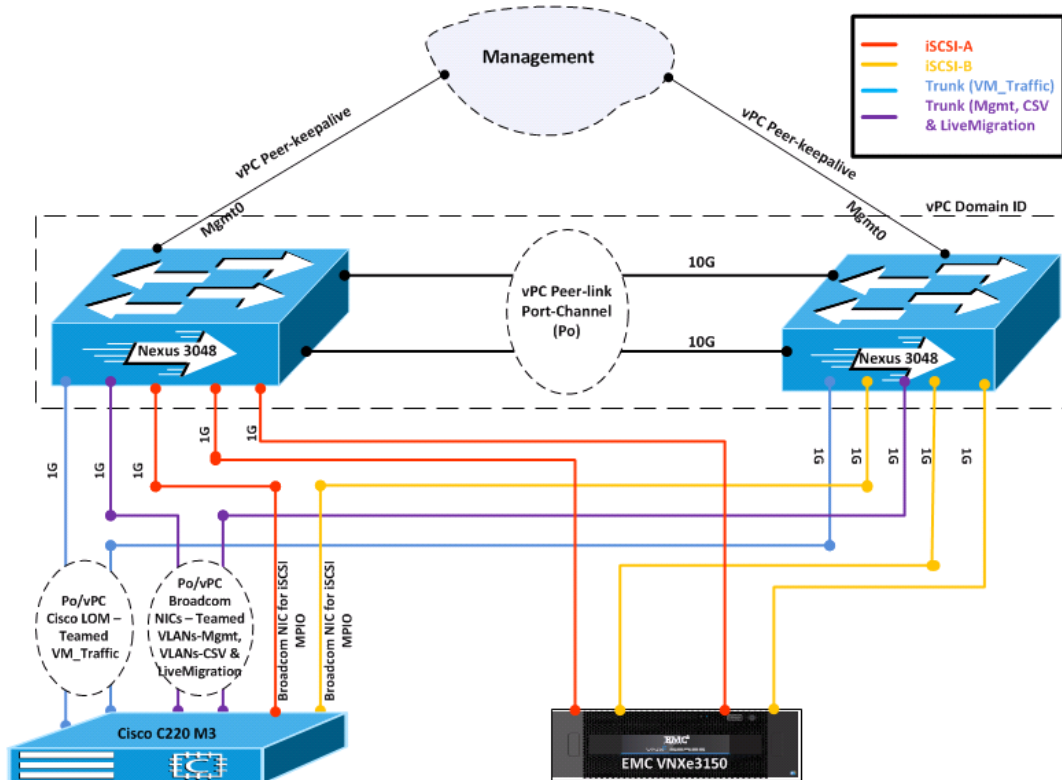
Figure 9 shows two switches configured for vPC. In vPC, a pair of switches acting as vPC peer endpoints looks like a single entity to port-channel-attached devices, although the two devices that act as logical port-channel endpoint are still two separate devices. This provides hardware redundancy with port-channel benefits. Both switches form a **vPC Domain**, in which one vPC switch is Primary while the other is secondary.



#### Note

The configuration steps detailed in this section provides guidance for configuring the Cisco Nexus 3048 running release 5.0(3)U2(2b).

**Figure 9** Network Configuration for EMC VSPEX M50



## Initial Setup of Nexus Switches

This section details the Cisco Nexus 3048 switch configuration for use in a VSPEX M50 environment.

On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start. This initial configuration addresses basic settings such as the switch name, the mgmt0 interface configuration, and SSH setup and defines the control plane policing policy.

## Initial Configuration of Cisco Nexus 3048 Switch A and B

**Figure 10** Initial Configuration

```

Abort Power On Auto Provisioning and continue with normal setup ?(yes/no)[n]: yes
----- System Admin Account Setup -----
Do you want to enforce secure password standard (yes/no): yes
Enter the password for "admin":*****
Confirm the password for "admin":*****
----- Basic System Configuration Dialog -----
Would you like to enter the basic configuration dialog (yes/no): y
Create another login account (yes/no) [n]:
Configure read-only SNMP community string (yes/no) [n]:
Configure read-write SNMP community string (yes/no) [n]:
Enter the switch name : Switch1
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
  Mgmt0 IPv4 address : 10.29.150.11
  Mgmt0 IPv4 netmask : 255.255.255.0
Configure the default gateway for mgmt? (yes/no) [y]:
  IPv4 address of the default gateway : 10.29.150.1
Enable the telnet service? (yes/no) [n]:
Enable the ssh service? (yes/no) [y]:
  Type of ssh key you would like to generate (dsa/rsa) : rsa
  Number of key bits <768-2048> : 1024
Configure the ntp server? (yes/no) [n]:
Configure CoPP System Policy Profile ( default / I2 / I3 ) [default]:

The following configuration will be applied:
switchname Switch1
interface mgmt0
ip address 10.29.150.11 255.255.255.0
no shutdown
exit
vrf context management
ip route 0.0.0.0/0 10.29.150.1
exit
no telnet server enable
ssh key rsa 1024 force
ssh server enable
policy-map type control-plane copp-system-policy ( default )

Use this configuration and save it? (yes/no) [y]:

```

## Software Upgrade (Optional)

It is always recommended to perform any required software upgrades on the switch at this point in the configuration. Download and install the latest available NX-OS software for the Cisco Nexus 3048 switch from the Cisco software download site. There are various methods to transfer both the NX-OS kickstart and system images to the switch. The simplest method is to leverage the USB port on the Switch. Download the NX-OS kickstart and system files to a USB drive and plug the USB drive into the external USB port on the Cisco Nexus 3048 switch.

Copy the files to the local bootflash and update the switch by using the following procedure.

**Figure 11** Procedure to update the Switch

```

copy usb1:<<kickstart_image_file>> bootflash:
copy usb1:<<system_image_file>> bootflash:
install all kickstart bootflash:<<kickstart_image_file>> system bootflash:<<system_image_file>>

```

## Enable Features

Enable certain advanced features within NX-OS. This is required for configuring some additional options. Enter configuration mode using the (config t) command, and type the following commands to enable the appropriate features on each switch.

### Enabling Features in Cisco Nexus 3048 Switch A and B

**Figure 12** *Command to Enable Features*

```
feature interface-vlan
feature lacp
feature vpc
```

## Global Port-Channel Configuration

The default port-channel load-balancing hash uses the source and destination IP to determine the load-balancing algorithm across the interfaces in the port channel. Better distribution across the members of the port channels can be achieved by providing more inputs to the hash algorithm beyond the source and destination IP. For this reason, adding the source and destination TCP port to the hash algorithm is highly recommended.

From configuration mode (config t), type the following commands to configure the global port-channel load-balancing configuration on each switch.

### Configuring Global Port-Channel Load-Balancing on Cisco Nexus Switch A and B

**Figure 13** *Commands to Configure Global Port-Channel and Load-Balancing*

```
port-channel load-balance ethernet source-dest-port
```

## Global Spanning-Tree Configuration

The Cisco Nexus platform leverages a new protection feature called bridge assurance. Bridge assurance helps to protect against a unidirectional link or other software failure and a device that continues to forward data traffic when it is no longer running the spanning-tree algorithm. Ports can be placed in one of a few states depending on the platform, including **network** and **edge**.

The recommended setting for bridge assurance is to consider all ports as network ports by default. From configuration mode (config t), type the following commands to configure the default spanning-tree options, including the default port type and BPDU guard on each switch.

### Configuring Global Spanning-Tree on Cisco Nexus Switch A and B

**Figure 14** *Configuring Spanning-Tree*

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

## Enable Jumbo Frames

Cisco solution for EMC VSPEX Microsoft Hyper-V architectures require MTU set at 9000 (jumbo frames) for efficient storage and live migration traffic. MTU configuration on Nexus 5000 series switches fall under global QoS configuration. You may need to configure additional QoS parameters as needed by the applications.

From configuration mode (config t), type the following commands to enable jumbo frames on each switch.

### Enabling Jumbo Frames on Cisco Nexus 3048 Switch A and B

**Figure 15**      **Enabling Jumbo Frames**

```
policy-map type network-qos jumbo
class type network-qos class-default
mtu 9000
system qos
service-policy type network-qos jumbo
```

## Configure VLANs

For VSPEX M50 configuration, create the layer 2 VLANs on both the Cisco Nexus 3048 Switches using the [Table 7](#) as reference. Create your own VLAN definition table with the help of “[Customer Configuration Data Sheet](#)” section on page 124.

From configuration mode (config t), type the following commands to define and describe the L2 VLANs.

**Table 7**      **Reference VLAN Definitions for EMC VSPEX Microsoft Hyper-V M50 Setup**

VLAN Name	VLAN Purpose	ID used in this document	Network Address	Host NICs in VLAN
iSCSI-A	For iSCSI-A traffic	20	10.10.20.0/24	1 Broadcom NIC
iSCSI-B	For iSCSI-B traffic	21	10.10.21.10/24	1 Broadcom NIC
For Cluster	For Cluster & CSV	24	10.10.24.0/24	2 Broadcom NICs in a team and on trunk link
CSV	For Live Migration	22	10.10.22.0/24	
LM	For VM data	23	10.10.23.0/24	2 Cisco 1GigE I350 LOM in team and on trunk link
Vm_Traffic	For Mgmt	1	10.29.150.0/24	

## Defining L2 VLANs on Cisco Nexus 3048 Switch A and B

**Figure 16** *Commands to Define L2 VLANs*

```
vlan <iscsi-a vlan_id>
name iscsi-a
vlan <iscsi-b vlan_id>
name iscsi-b
vlan <livemigration vlan_id>
name livemigration
vlan <cluster-csv vlan_id>
name cluster-csv
vlan <vm_traffic vlan_id>
name vm_traffic
```

## Ethernet Interface Port Descriptions

This section shows the steps to set descriptions on all the interfaces.

**Figure 17** *Descriptions on All the Interfaces*

interface Ethernet 1/3 description Server-1 Intel mLOM NIC1-VM_Traffic	interface Ethernet 1/3 description Server-1 Intel mLOM NIC2-VM_Traffic
interface Ethernet 1/4 description Server-2 Intel mLOM NIC1-VM_Traffic	interface Ethernet 1/4 description Server-2 Intel mLOM NIC2-VM_Traffic
interface Ethernet 1/5 description Server-3 Intel mLOM NIC1-VM_Traffic	interface Ethernet 1/5 description Server-3 Intel mLOM NIC2-VM_Traffic
interface Ethernet 1/9 description Infrastructure network	interface Ethernet 1/9 description Infrastructure network
interface Ethernet 1/10 description Infrastructure network	interface Ethernet 1/10 description Infrastructure network
interface Ethernet 1/13 description Server-1 Broadcom NIC1-ISCSI-A	interface Ethernet 1/13 description Server-1 Broadcom NIC2-ISCSI-B
interface Ethernet 1/14 description Server-1 Broadcom NIC3-Mgmt/Cluster	interface Ethernet 1/14 description Server-1 Broadcom NIC4-Mgmt/Cluster
interface Ethernet 1/15 description Server-2 Broadcom NIC1-ISCSI-A	interface Ethernet 1/15 description Server-2 Broadcom NIC2-ISCSI-B
interface Ethernet 1/16 description Server-2 Broadcom NIC3-Mgmt/Cluster	interface Ethernet 1/16 description Server-2 Broadcom NIC4-Mgmt/Cluster
interface Ethernet 1/17 description Server-3 Broadcom NIC1-ISCSI-A	interface Ethernet 1/17 description Server-3 Broadcom NIC2-ISCSI-B
interface Ethernet 1/18 description Server-3 Broadcom NIC3-Mgmt/Cluster	interface Ethernet 1/18 description Server-3 Broadcom NIC4-Mgmt/Cluster
interface Ethernet 1/25 description VNXe3150 SPA:eth10	interface Ethernet 1/25 description VNXe3150 SPA:eth11
interface Ethernet 1/26 description VNXe3150 SPB:eth10	interface Ethernet 1/26 description VNXe3150 SPB:eth11
interface Ethernet 1/51 description vPC peer-link Switch2:1/51	interface Ethernet 1/51 description vPC peer-link Switch1:1/51
interface Ethernet 1/52 description vPC peer-link Switch2:1/52	interface Ethernet 1/52 description vPC peer-link Switch1:1/52

## Virtual Port-Channel (vPC) Global Configuration

The vPC feature requires an initial setup between the two Cisco Nexus switches to function properly. From configuration mode (config t), type the following commands to configure the vPC global configuration for Switch A.

## Configuring vPC Global on Cisco Nexus Switch A

**Figure 18** Commands to Configure vPC Global Configuration on Switch A

```
vpc domain 101
role priority 10
peer-keepalive destination <mgmt0_ip_address of switch2>

int eth1/51-52
channel-group 10 mode active

int Po10
description vPC peer-link
switchport mode trunk
switchport trunk allowed vlan 1, <iscsia_vlan_id>, <iscsib_vlan_id>,
<livemigration_vlan_id>, <csv_vlan_id>, <vmtraffic_vlan_id>
spanning-tree port type network
vpc peer-link
no shut
```

From configuration mode (config t), type the following commands to configure the vPC global configuration for Switch B.

## Configuring vPC Global on Cisco Nexus Switch B

**Figure 19** Commands to Configure vPC Global Configuration on Switch B

```
vpc domain 101
role priority 10
peer-keepalive destination <mgmt0_ip_address of switch1>

int eth1/51-52
channel-group 10 mode active

int Po10
description vPC peer-link
switchport mode trunk
switchport trunk allowed vlan 1, <iscsia_vlan_id>, <iscsib_vlan_id>,
<livemigration_vlan_id>, <csv_vlan_id>, <vmtraffic_vlan_id>
spanning-tree port type network
vpc peer-link
no shut
```

## Storage Connections Configuration

Switch interfaces connected to the VNXe storage ports are configured as access ports. Each controller will have two links to each switch.

From the configuration mode (config t), type the following commands on each switch to configure the individual interfaces.



## Cisco Nexus 3048 Switch A with VNxe SPA configuration

**Figure 20**      *Commands to Configure VNxe Interface on Switch A*

```
interface Ethernet1/25
description VNxe3150 SPA:eth10
switchport access vlan 20
spanning-tree port type edge
no shut

interface Ethernet1/26
description VNxe3150 SPB:eth10
switchport access vlan 20
spanning-tree port type edge
no shut
```

## Cisco Nexus 3048 Switch B with VNxe SPA configuration

**Figure 21**      *Commands to Configure VNxe Interface on Switch B*

```
interface Ethernet1/25
description VNxe3150 SPA:eth11
switchport access vlan 21
spanning-tree port type edge
no shut

interface Ethernet1/26
description VNxe3150 SPB:eth11
switchport access vlan 21
spanning-tree port type edge
no shut
```

## Server Connections Configurations

Each server has six network adapters (two Intel and four Broadcom ports) connected to both switches for redundancy as shown in [Figure 9](#). This section provides the steps to configure the interfaces on both the switches that are connected to the servers.



## Cisco Nexus Switch A with Server 1 configuration

**Figure 22**      *Commands to Configure Interface on Switch A for Server 1 Connectivity*

```
interface Ethernet1/3
description Server-1 Intel mLOM NIC1-VM_Traffic
channel-group 3 mode active

interface port-channel3
switchport mode trunk
switchport trunk allowed vlan 1,<vm_traffic_vlan_id>
spanning-tree port type edge
vpc 3
no shut

interface Ethernet1/13
description Server-1 Broadcom NIC1-ISCSI-A
switchport access vlan 20
spanning-tree port type edge
no shut

interface Ethernet1/14
description Server-1 Broadcom NIC3-Mgmt/Cluster
channel-group 14 mode active

interface port-channel14
switchport mode trunk
switchport trunk allowed vlan 1,<cluster_csv_vlan_id>,<livemigration_vlan_id>
spanning-tree port type edge
vpc 14
no shut
```

## Cisco Nexus Switch B with Server 1 configuration

**Figure 23**      *Commands to Configure Interface on Switch B and Server 1 Connectivity*

```
interface Ethernet1/3
description Server-1 Intel mLOM NIC2-VM_Traffic
channel-group 3 mode active

interface port-channel3
switchport mode trunk
switchport trunk allowed vlan 1,<vm_traffic_vlan_id>
spanning-tree port type edge
vpc 3
no shut

interface Ethernet1/13
description Server-1 Broadcom NIC2-ISCSI-B
switchport access vlan 21
spanning-tree port type edge
no shut

interface Ethernet1/14
description Server-1 Broadcom NIC4-Mgmt/Cluster
channel-group 14 mode active

interface port-channel14
switchport mode trunk
switchport trunk allowed vlan 1,<cluster_csv_vlan_id>,<livemigration_vlan_id>
spanning-tree port type edge
vpc 14
no shut
```

## Cisco Nexus Switch A with Server 2 configuration

**Figure 24**      *Commands to Configure Interface on Switch A and Server 2 Connectivity*

```
interface Ethernet1/4
description Server-2 Intel mLOM NIC1-VM_Traffic
channel-group 4 mode active

interface port-channel4
switchport mode trunk
switchport trunk allowed vlan 1,<vm_traffic_vlan_id>
spanning-tree port type edge
vpc 4
no shut

interface Ethernet1/15
description Server-2 Broadcom NIC1-iSCSI-A
switchport access vlan 20
spanning-tree port type edge
no shut

interface Ethernet1/16
description Server-2 Broadcom NIC3-Mgmt/Cluster
channel-group 16 mode active

interface port-channel16
switchport mode trunk
switchport trunk allowed vlan 1,<cluster_csv_vlan_id>,<livemigration_vlan_id>
spanning-tree port type edge
vpc 16
no shut
```

## Cisco Nexus Switch B with Server 2 configuration

**Figure 25**      *Commands to Configure Interface on Switch B and Server 2 Connectivity*

```
interface Ethernet1/4
description Server-2 Intel mLOM NIC2-VM_Traffic
channel-group 4 mode active

interface port-channel4
switchport mode trunk
switchport trunk allowed vlan 1,<vm_traffic_vlan_id>
spanning-tree port type edge
vpc 4
no shut

interface Ethernet1/15
description Server-2 Broadcom NIC2-iSCSI-B
switchport access vlan 21
spanning-tree port type edge
no shut

interface Ethernet1/16
description Server-2 Broadcom NIC4-Mgmt/Cluster
channel-group 16 mode active

interface port-channel16
switchport mode trunk
switchport trunk allowed vlan 1,<cluster_csv_vlan_id>,<livemigration_vlan_id>
spanning-tree port type edge
vpc 16
no shut
```

## Cisco Nexus Switch A with Server 3 configuration

**Figure 26** Commands to Configure Interface on Switch A and Server 3 Connectivity

```
interface Ethernet1/5
description Server-3 Intel mLOM NIC1-VM_Traffic
channel-group 5 mode active

interface port-channel5
switchport mode trunk
switchport trunk allowed vlan 1,<vm_traffic_vlan_id>
spanning-tree port type edge
vpc 5
no shut

interface Ethernet1/17
description Server-3 Broadcom NIC1-ISCSI-A
switchport access vlan 20
spanning-tree port type edge
no shut

interface Ethernet1/18
description Server-3 Broadcom NIC3-Mgmt/Cluster
channel-group 18 mode active

interface port-channel18
switchport mode trunk
switchport trunk allowed vlan 1,<cluster-csv_vlan_id>,<livemigration_vlan_id>
spanning-tree port type edge
vpc 18
no shut
```

## Cisco Nexus Switch B with Server 3 configuration

**Figure 27** Commands to Configure Interface on Switch B and Server 3 Connectivity

```
interface Ethernet1/5
description Server-3 Intel mLOM NIC2-VM_Traffic
channel-group 5 mode active

interface port-channel5
switchport mode trunk
switchport trunk allowed vlan 1,<vm_traffic_vlan_id>
spanning-tree port type edge
vpc 5
no shut

interface Ethernet1/17
description Server-3 Broadcom NIC2-ISCSI-B
switchport access vlan 21
spanning-tree port type edge
no shut

interface Ethernet1/18
description Server-3 Broadcom NIC4-Mgmt/Cluster
channel-group 18 mode active

interface port-channel18
switchport mode trunk
switchport trunk allowed vlan 1,<cluster-csv_vlan_id>,<livemigration_vlan_id>
spanning-tree port type edge
vpc 18
no shut
```

At this point, all the ports and port-channels are configured with necessary VLANs, switchport mode and vPC configuration. Validate this configuration using the **show port-channel summary** and **show vlan brief** commands as shown in [Figure 28](#) and [Figure 29](#).

**Figure 28**      **Show vlan brief**

```

N3048A# sh vlan brief
VLAN Name                Status    Ports
-----
1  default                 active    Po3, Po4, Po5, Po10, Po14, Po16
                                Po18, Eth1/1, Eth1/2, Eth1/5
                                Eth1/6, Eth1/7, Eth1/8, Eth1/9
                                Eth1/10, Eth1/11, Eth1/12
                                Eth1/18, Eth1/19, Eth1/20
                                Eth1/21, Eth1/22, Eth1/23
                                Eth1/24, Eth1/27, Eth1/28
                                Eth1/29, Eth1/30, Eth1/31
                                Eth1/32, Eth1/33, Eth1/34
                                Eth1/35, Eth1/36, Eth1/37
                                Eth1/38, Eth1/39, Eth1/40
                                Eth1/41, Eth1/42, Eth1/43
                                Eth1/44, Eth1/45, Eth1/46
                                Eth1/47, Eth1/48, Eth1/49
                                Eth1/50
20  ISCSI-A                 active    Po3, Po4, Po5, Po10, Po14, Po16
                                Po18, Eth1/1, Eth1/5, Eth1/9
                                Eth1/10, Eth1/12, Eth1/13
                                Eth1/15, Eth1/17, Eth1/18
                                Eth1/25, Eth1/26
21  ISCSI-B                 active    Po3, Po4, Po5, Po10, Po14, Po16
                                Po18, Eth1/1, Eth1/5, Eth1/9
                                Eth1/10, Eth1/12, Eth1/18
22  LiveMigration            active    Po3, Po4, Po5, Po10, Po14, Po16
                                Po18, Eth1/1, Eth1/5, Eth1/9
                                Eth1/10, Eth1/12, Eth1/18
23  VM_Traffic               active    Po3, Po4, Po5, Po10, Po14, Po16
                                Po18, Eth1/1, Eth1/5, Eth1/9
                                Eth1/10, Eth1/12, Eth1/18
24  Cluster-CSV              active    Po3, Po4, Po5, Po10, Po14, Po16
                                Po18, Eth1/1, Eth1/5, Eth1/9
                                Eth1/10, Eth1/12, Eth1/18

```

Ensure that on both switches, all required VLANs are in active status and right set of ports and port-channels are part of the necessary VLANs.

Port-channel configuration can be verified using **show port-channel summary** command. [Figure 29](#) shows the expected output of this command after completing the NIC teaming of Ethernet interfaces on the host covered in “[Network Configuration](#)” section on [page 45](#).

**Figure 29**      **Show Port-Channel Summary Output**

```

N3048A(config-if)# sh port-channel summary
Flags: D - Down      P - Up in port-channel (members)
       I - Individual H - Hot-standby (LACP only)
       s - Suspended  r - Module-removed
       S - Switched   R - Routed
       U - Up (port-channel)

Group Port-Channel  Type  Protocol  Member Ports
-----
3  Po3(SU)           Eth    LACP      Eth1/3(P)
4  Po4(SU)           Eth    LACP      Eth1/4(P)
5  Po5(SU)           Eth    LACP      Eth1/5(P)
10 Po10(SU)           Eth    LACP      Eth1/51(P) Eth1/52(P)
14 Po14(SU)          Eth    LACP      Eth1/14(P)
16 Po16(SU)          Eth    LACP      Eth1/16(P)
18 Po18(SU)          Eth    LACP      Eth1/18(P)

```

In this example, port-channel 10 is the vPC peer-link port-channel, port-channels 3, 4 and 5 are connected to the Cisco 1GigE I350 LOM on the host and port-channels 14, 16 and 18 are connected to the Broadcom NICs on the host. Make sure that state of the member ports of each port-channel is “P” (Up in port-channel). Note that port may not come up if the peer ports are not properly configured. Common reasons for port-channel port being down are:

- Port-channel protocol mis-match across the peers (LACP v/s none)

- Inconsistencies across two vPC peer switches. Use **show vpc consistency-parameters {global | interface {port-channel | port} <id>}** command to diagnose such inconsistencies.

vPC status can be verified using **show vpc brief** command. Example output is shown in [Figure 30](#):

**Figure 30**      **Show vpc Brief Output**

```
N3048A# sh vpc brief
Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 101
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                : secondary
Number of vPCs configured : 6
Peer Gateway            : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled

vPC Peer-link status
-----
id  Port  Status Active vlans
-----
1   Po10  up    1,20-24

vPC status
-----
id  Port  Status Consistency Reason  Active vlans
-----
3   Po3   up    success  success  1,23
4   Po4   up    success  success  1,23
5   Po5   up    success  success  1,23
14  Po14   up    success  success  1,22,24
16  Po16   up    success  success  1,22,24
18  Po18   up    success  success  1,22,24
```

Make sure that vPC peer status is peer adjacency formed ok and all the port-channels, including the peer-link port-channel, have status up.

## Infrastructure Servers

Most environments will already have DNS and Active Directory services in their infrastructure either running on a virtual machine or on a physical server. This section will not cover the installation and configuration of DNS and Active Directory Domain Controllers.

## Prepare the Cisco UCS C220 M3 Servers

This section provides the detailed procedure for configuring a Cisco Unified Computing System C-Series standalone server for use in VSPEX M50 configurations. Perform all the steps mentioned in this section on all the hosts.

## Configure Cisco Integrated Management Controller (CIMC)

These steps describe the setup of the initial Cisco UCS C-Series standalone server. Follow these steps on all servers:

1. Attach a supplied power cord to each power supply in your server, and then attach the power cord to a grounded AC power outlet.
2. Connect a USB keyboard and VGA monitor by using the supplied KVM cable connected to the KVM connector on the front panel.
3. Press the **Power** button to boot the server. Watch for the prompt to press F8.
4. During bootup, press **F8** when prompted to open the BIOS CIMC Configuration Utility.
5. Set the **NIC mode** to **Dedicated** and **NIC redundancy** to **None**.
6. Choose whether to enable DHCP for dynamic network settings, or to enter static network settings.
7. Press F10 to save your settings and reboot the server.

**Figure 31** *CIMC Configuration Utility*

```

CIMC Configuration Utility  Version 1.5  Cisco Systems, Inc.
*****
NIC Properties
NIC mode                               NIC redundancy
Dedicated:      [X]                   None:          [X]
Shared LOM:     [ ]                   Active-standby:[ ]
Shared LOM 10G: [ ]                   Active-active: [ ]
Cisco Card:     [ ]

IPV4 (Basic)                            Factory Defaults
DHCP enabled:   [ ]                   CIMC Factory Default:[ ]
CIMC IP:        10.29.150.101         Default User (Basic)
Subnetmask:     255.255.255.0         Default password:
Gateway:        10.29.150.1          Reenter password:

VLAN (Advanced)
VLAN enabled:   [ ]
VLAN ID:        1
Priority:        0

*****
<Up/Down arrow> Select items    <F10> Save    <Space bar> Enable/Disable
<F5> Refresh                    <ESC> Exit

```

Once the CIMC IP is configured, the server can be managed using the https based Web GUI or CLI.



### Note

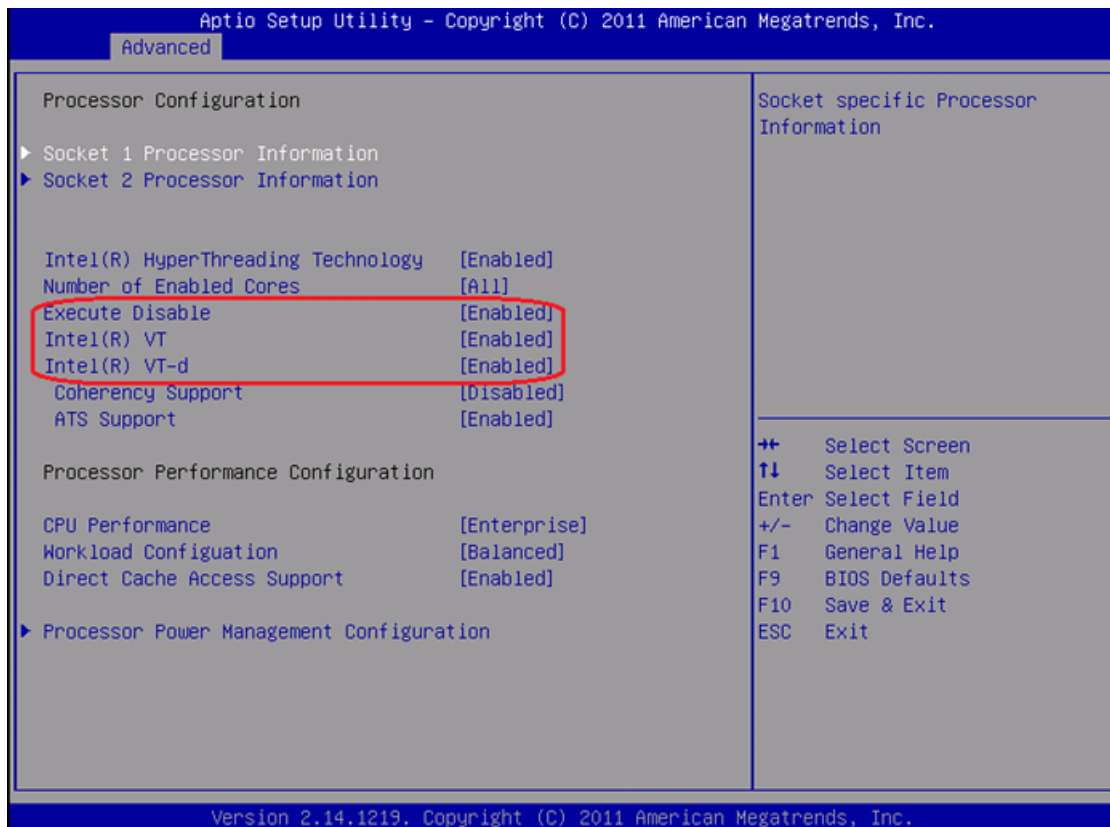
The default username for the server is “admin” and the default password is “password”. Cisco strongly recommends changing the default password.

## Enabling Virtualization Technology in BIOS

Hyper-V requires an x64-based processor, hardware-assisted virtualization (Intel VT enabled), and hardware data execution protection (Execute Disable enabled). Follow these steps on all the servers to enable Intel ® VT and Execute Disable in BIOS:

1. Press the **Power** button to boot the server. Watch for the prompt to press **F2**.
2. During bootup, press **F2** when prompted to open the BIOS Setup Utility.
3. Choose the **Advanced** tab > **Processor Configuration**.

**Figure 32** Cisco UCS C220 M3 KVM Console



4. Enable **Execute Disable** and **Intel VT** as shown in [Figure 32](#).

## Configuring RAID

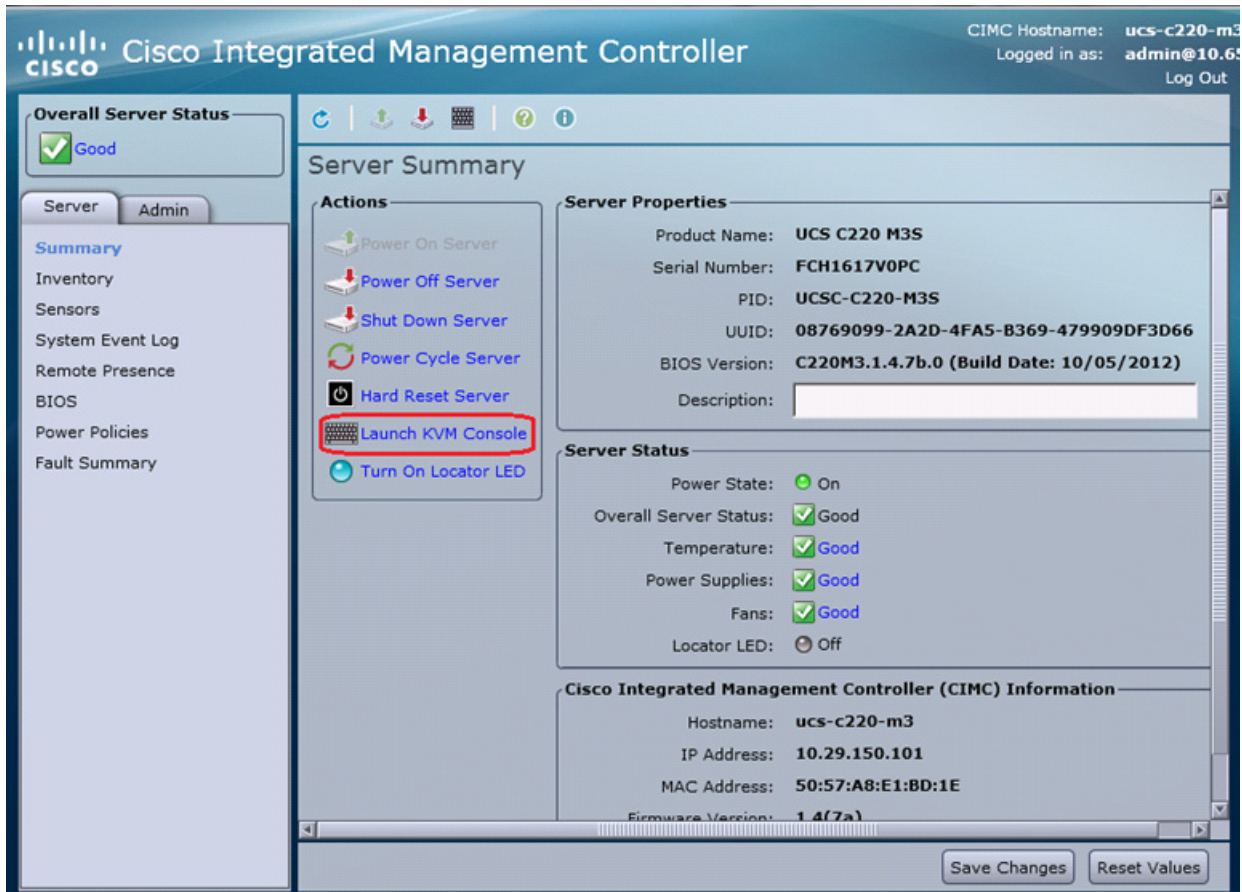
The RAID controller type is Cisco UCSC RAID SAS 2008 and supports 0, 1, 5 RAID levels. We need to configure RAID level 1 for this setup and set the virtual drive as boot drive.

To configure RAID controller, follow these steps on all the servers:

1. Using a web browser, connect to the CIMC using the IP address configured in the CIMC Configuration section.
2. Launch the KVM from the CIMC GUI.

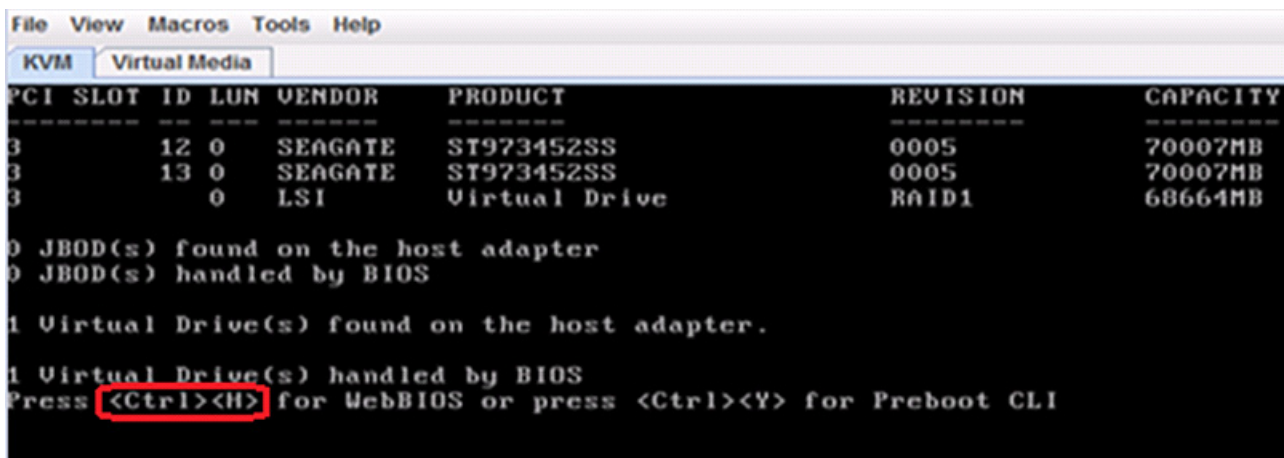


Figure 33 Cisco UCS C220 M3 CIMC GUI



- During bootup, press <Ctrl> <H> when prompted to configure RAID in the WebBIOS.

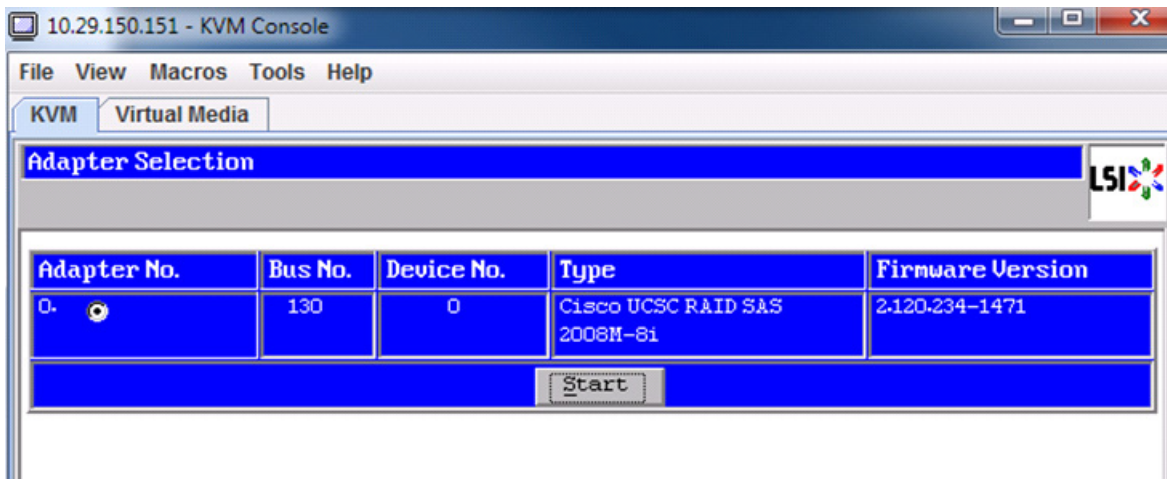
Figure 34 Cisco UCS C220 M3 KVM Console - Server Booting



- Select the adapter and click **Start**.

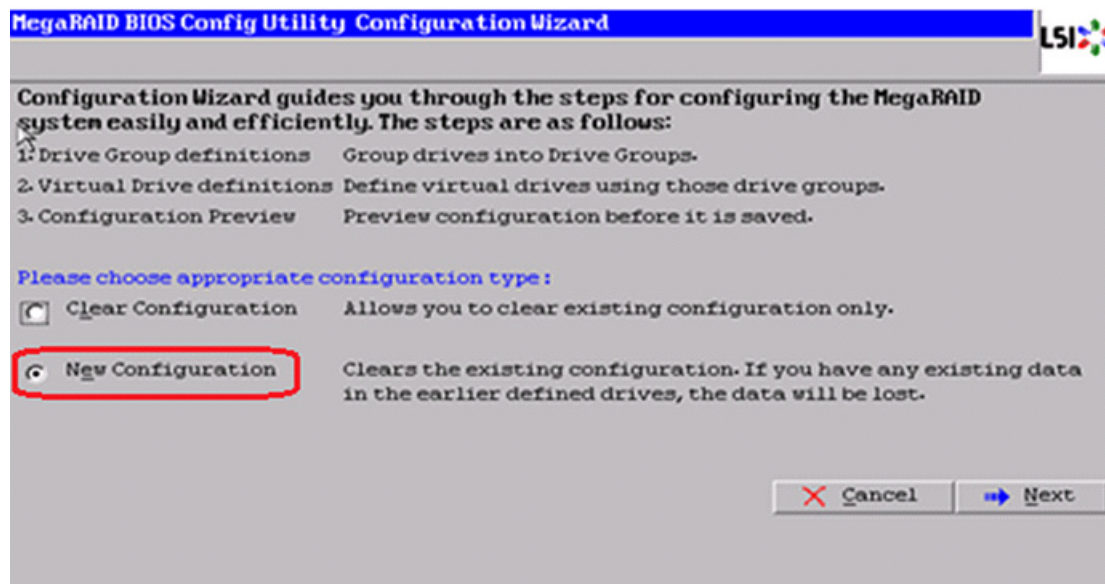


**Figure 35 Adapter Selection for RAID Configuration**



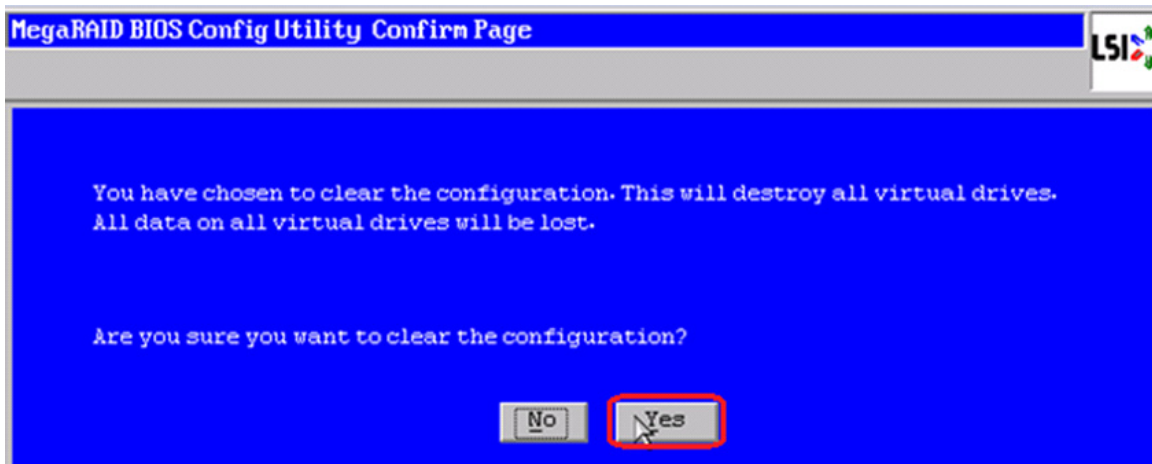
- Click **New Configuration** and click **Next**.

**Figure 36 MegaRAID BIOS Config Utility Configuration Wizard**



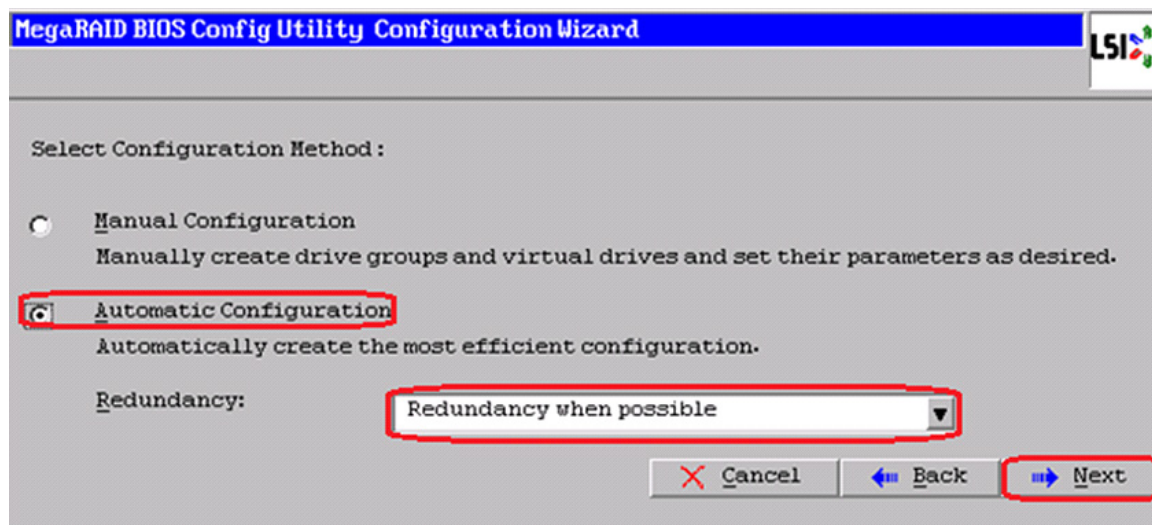
- Select **Yes** and click **Next** to clear the configuration.

Figure 37 MegaRAID BIOS Config Utility Confirmation Page



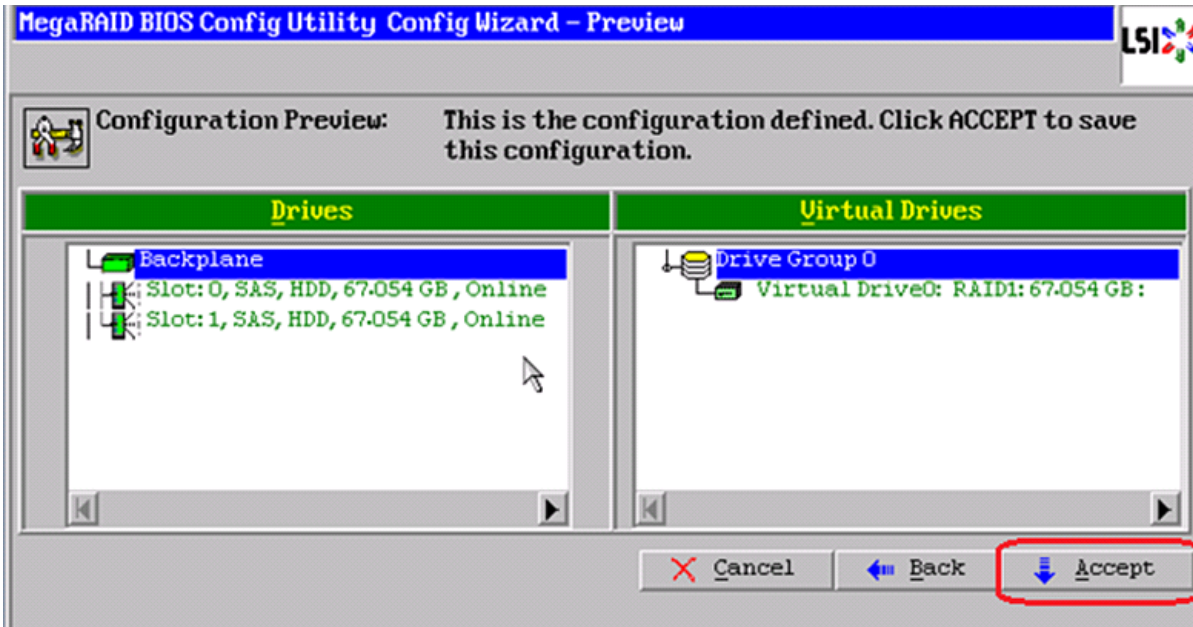
7. If you click **Automatic Configuration** radio button and **Redundancy when possible** for Redundancy and only two drives are available, WebBIOS creates a RAID 1 configuration.

Figure 38 MegaRAID BIOS Config Utility Configuration Wizard - Select Configuration Method



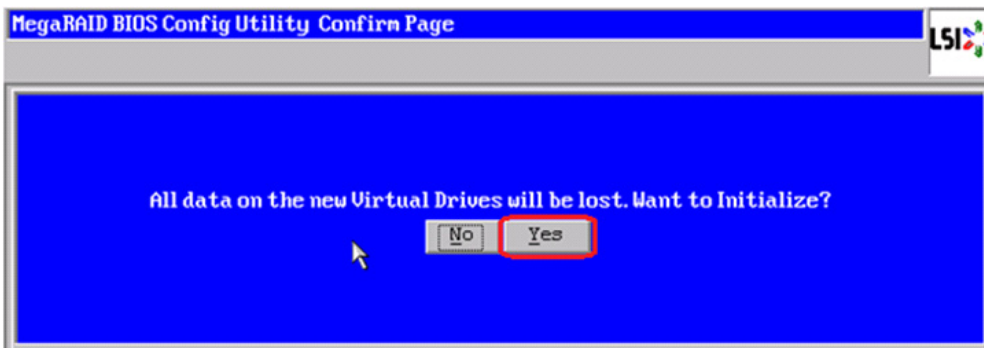
8. Click **Accept** when you are prompted to save the configuration.

Figure 39 MegaRAID BIOS Config Utility Config Wizard - Preview



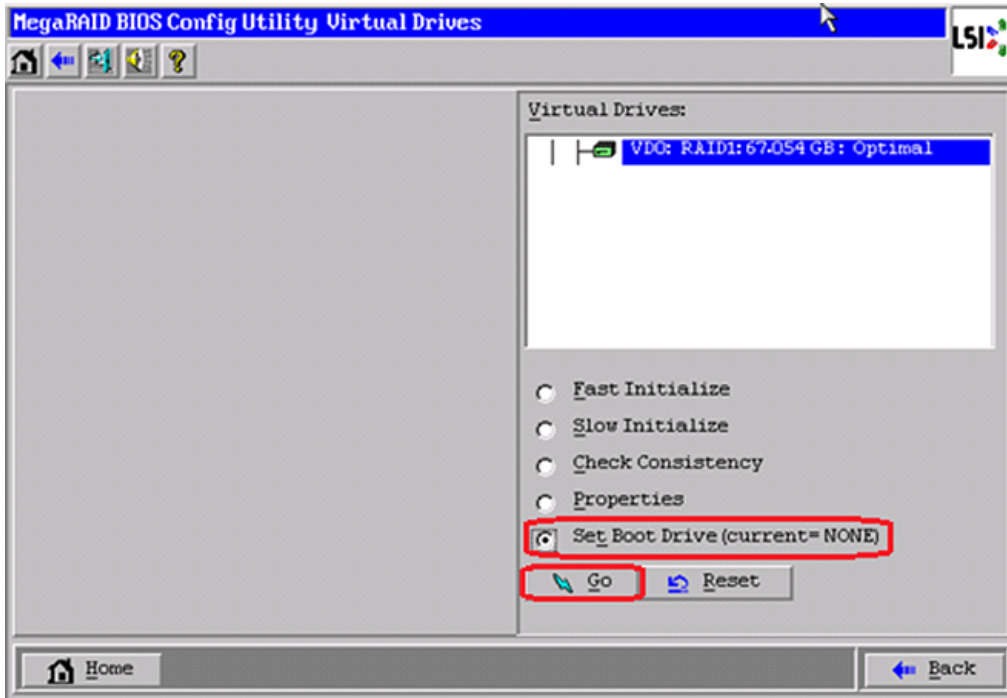
9. Click **Yes** when prompted to initialize the new virtual drives.

Figure 40 MegaRAID BIOS Config Utility Confirmation Page



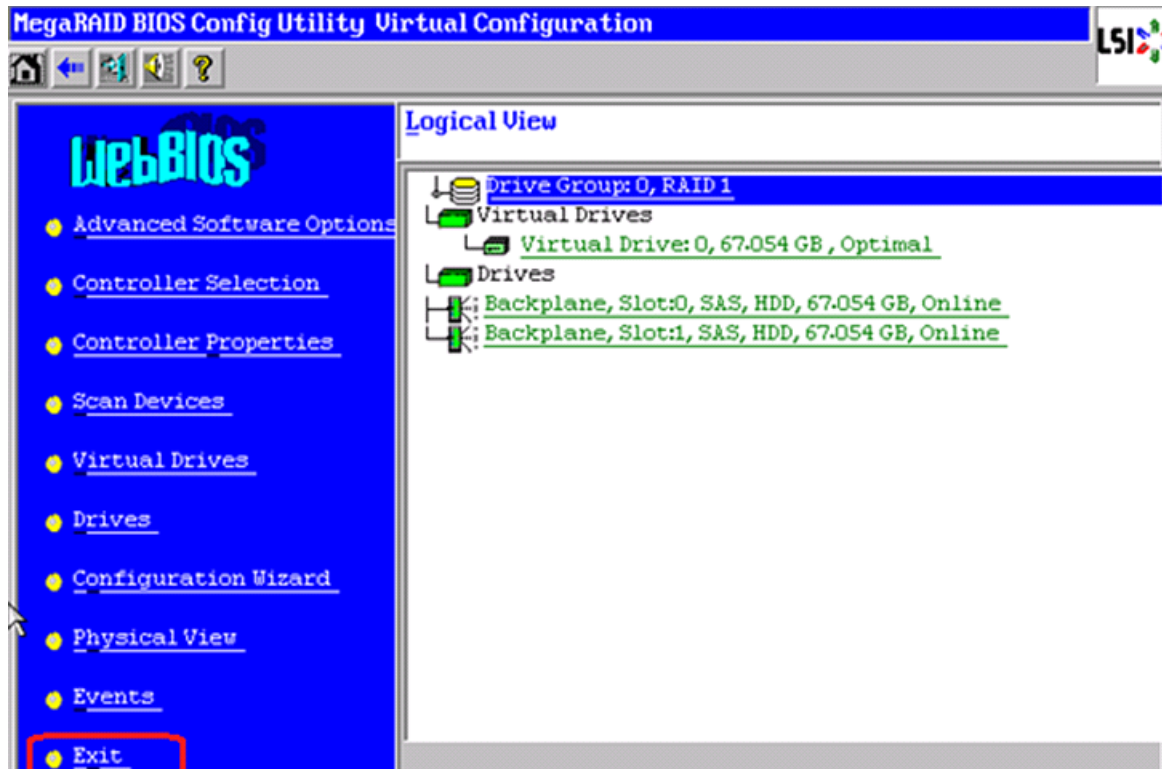
10. Click the **Set Boot Drive** radio button for the virtual drive created above and click **GO**.

Figure 41 MegaRAID BIOS Config Utility Virtual Drives



11. Click **Exit** and reboot the system.

Figure 42 MegaRAID BIOS Config Utility Virtual Configuration



## Install Microsoft Windows Server 2012 on Cisco UCS C220 M3 Servers

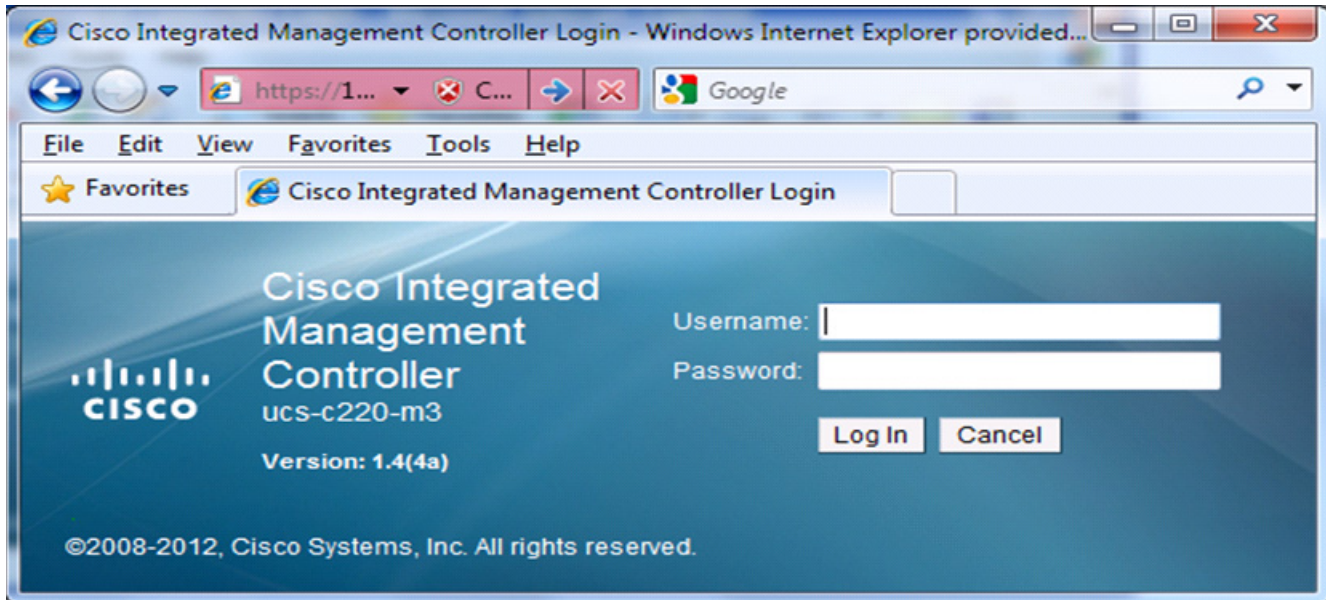
This section provides detailed procedures for installing Windows Server 2012 in an M50 VSPEX configuration. Multiple methods exist for installing Windows Server in such an environment. This procedure highlights using the virtual KVM console and virtual media features within the Cisco UCS C-Series CIMC interface to map remote installation media to each individual server.

### Connect and log into the Cisco UCS C-Series Standalone Server CIMC Interface

1. Open a web browser and enter the IP address for the Cisco UCS C-series CIMC interface. This will launch the CIMC GUI application
2. Log in to CIMC GUI with admin user name and credentials.

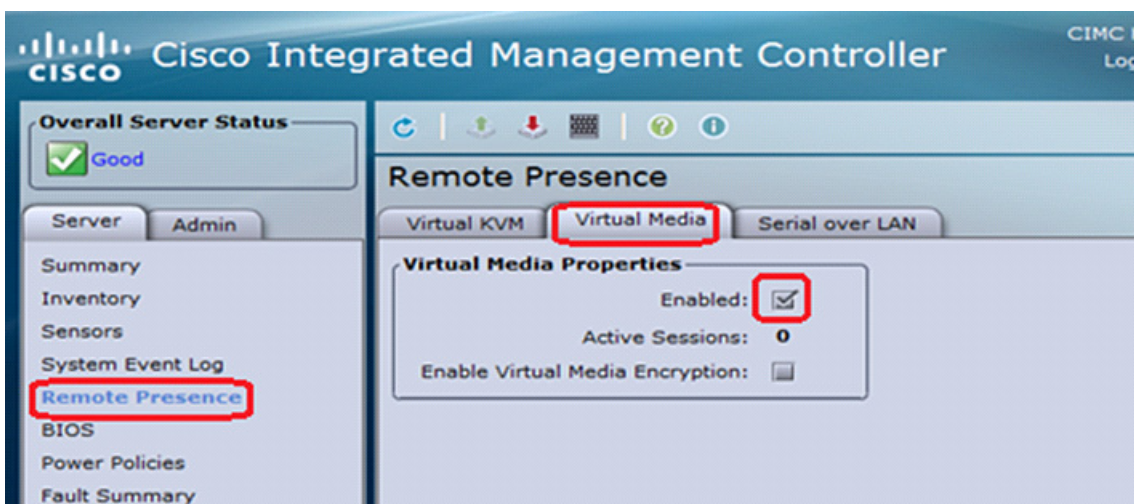


**Figure 43** *CIMC Manager Login Page*



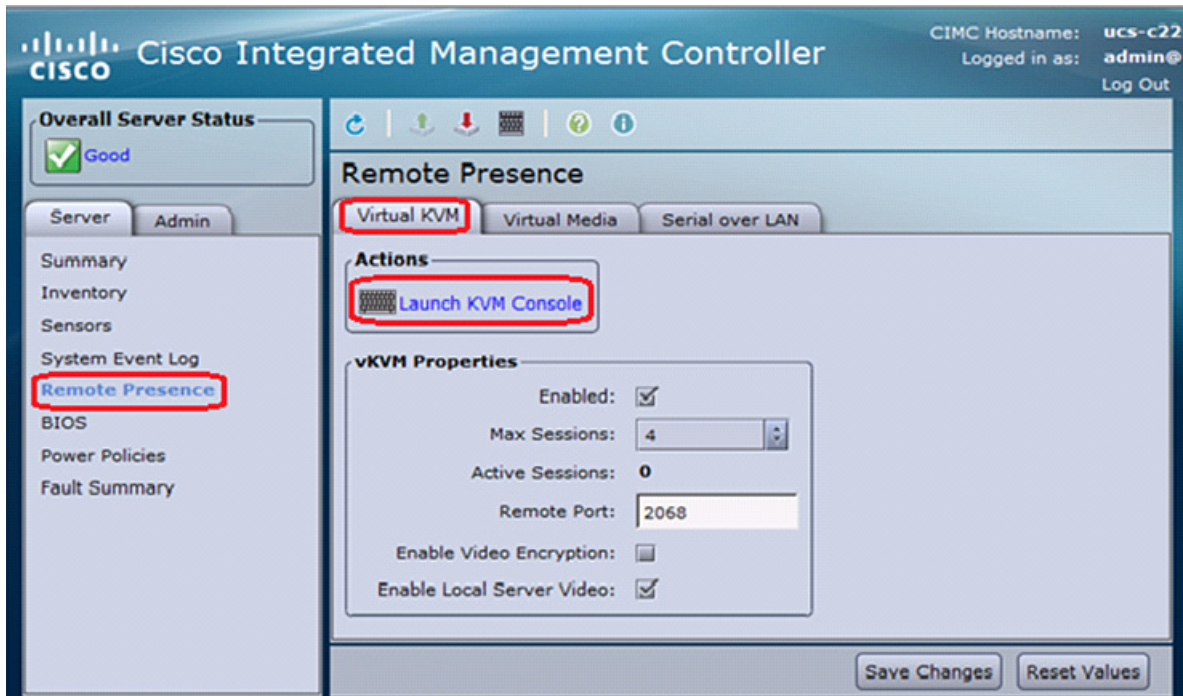
3. In the home page, choose the **Server** tab.
4. Click **launch KVM Console**.
5. Enable the Virtual Media feature, which enables the server to mount virtual drives:
  - a. In the CIMC Manager Server tab, click **Remote Presence**.
  - b. In the Remote Presence window, click the **Virtual Media** tab and check the check box to enable Virtual Media.
  - c. Click **Save Changes**.

**Figure 44** *CIMC Manager Remote Presence - Virtual Media*



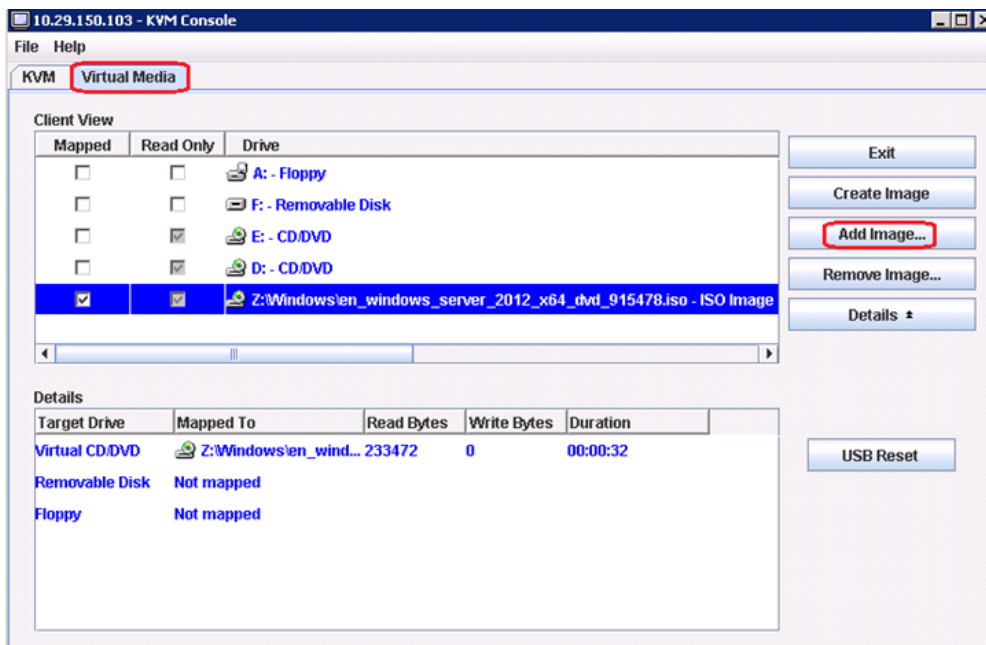
6. On the Remote Presence window, click the **Virtual KVM** tab and then click **Launch KVM Console**.

Figure 45 CIMC Manager Remote Presence - Virtual KVM



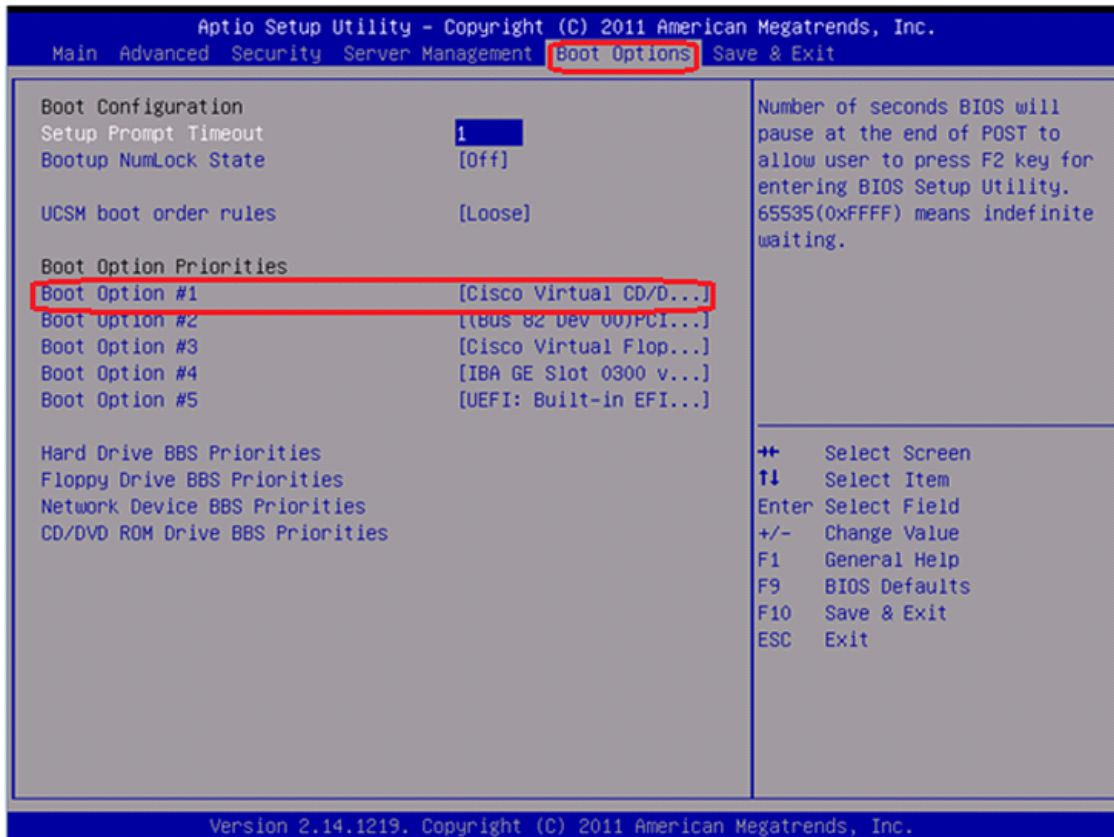
7. When the Virtual KVM Console window launches, click the **Virtual Media** tab.
8. In the Virtual Media Session window, provide the path to the Windows installation image by clicking **Add Image** and then use the dialog to navigate to your Windows Server 2012 ISO file and select it. The ISO image is displayed in the Client View pane.

Figure 46 CIMC Manager Virtual Media - Add Image



9. When mapping is complete, power cycle the server so that the BIOS recognizes the media that you just added.
10. In the Virtual KVM Console window, watch during bootup for the F2 prompt, and then press **F2** to enter BIOS setup. Wait for the setup utility screen to appear.
11. On the BIOS Setup utility screen, choose the **Boot Options** tab and verify that you see the virtual DVD device that you just added in the above step 8 listed as a bootable device and move it up to the top under Boot Option Priorities as shown in [Figure 47](#).

**Figure 47** Cisco UCS C220 M3 BIOS Setup Utility



12. Exit the BIOS Setup utility and restart the server.

## Install Windows Server 2012

1. The Windows installation begins when the image is booted.
2. Press **Enter** when prompted to boot from CD.
3. After the installer is finished loading, enter the relevant region information and click **Next**.
4. Click **Install now**.
5. Enter the product key and click **Next**.
6. Select Windows Server 2012 Datacenter (Server with a GUI) and click **Next**.
7. After reviewing the EULA, select **I accept the license terms** and click **Next**.



8. Choose Custom: Install Windows only (advanced).
9. Choose the local RAID drive that was set up previously as the installation location for Windows. Click **Next**.
10. After the installation is complete, be sure to unmap the Windows installation image in the virtual media tab of the KVM Console so that the server reboots into Windows and not the installer.
11. The Virtual Media window might warn you that it is preferable to eject the media from the guest. Because we cannot do this (and the media is read-only), unmap the image anyway by clicking **Yes**.
12. Back in the KVM tab; press **Enter** to reboot the server.
13. When Windows is finished installing, enter an administrator password on the settings page and click **Finish**.
14. Download the latest drivers if any available from the following link and install them:  
<http://software.cisco.com/download/type.html?mdfid=284296253&flowid=31742>

## Network Configuration

To configure the network for each Hyper-V host, follow these steps:

1. Log in with the administrator password previously entered during installation.
2. Launch a Windows PowerShell prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.
3. (Optional) For easy identification and to match per its intended use, rename the network adapters as shown below.

```
Rename-NetAdapter -InterfaceAlias <Ethernet> -NewName <Mgmt-Member1>
Rename-NetAdapter -InterfaceAlias <"Ethernet 3"> -NewName <Mgmt-Member2>
Rename-NetAdapter -InterfaceAlias <"Ethernet 6"> -NewName <VM-Member1>
Rename-NetAdapter -InterfaceAlias <"Ethernet 5"> -NewName <VM-Member2>
Rename-NetAdapter -InterfaceAlias <"Ethernet 2"> -NewName <iSCSI-A>
Rename-NetAdapter -InterfaceAlias <"Ethernet 4"> -NewName <iSCSI-B>
```



**Note**

Because of how Windows Plug and Play detects hardware, your list will most likely change. You will have to physically identify which port is connected to each server by disconnecting the link.

4. Configure jumbo frames on the NICs carrying Storage and Live Migration traffic.

```
Set-NetAdapterAdvancedProperty -Name
<Mgmt-Member1,Mgmt-Member2,VM-Member1,VM-Member2> -DisplayName "Jumbo
Packet" -DisplayValue "9014 Bytes" -EA SilentlyContinue

Set-NetAdapterAdvancedProperty -Name
<Mgmt-Member1,Mgmt-Member2,VM-Member1,VM-Member2> -DisplayName "Jumbo
Packet" -DisplayValue "9014" -EA SilentlyContinue
```



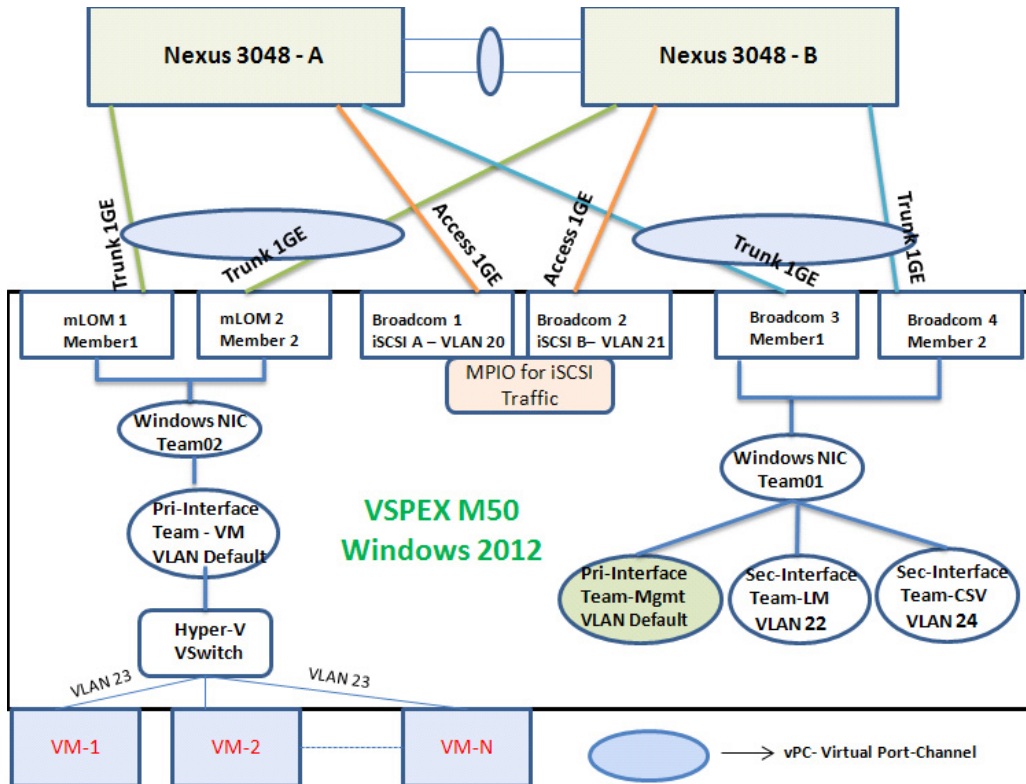
**Note**

The first command changes the jumbo frame setting on Intel NICs and the second command changes the setting on Broadcom NICs.

5. Configure NIC Teaming.

NIC teaming is done using the in-built Windows 2012 NIC Teaming feature (also known as Load Balancing/Failover - LBFO) for bandwidth aggregation and redundancy in case of a component failure.

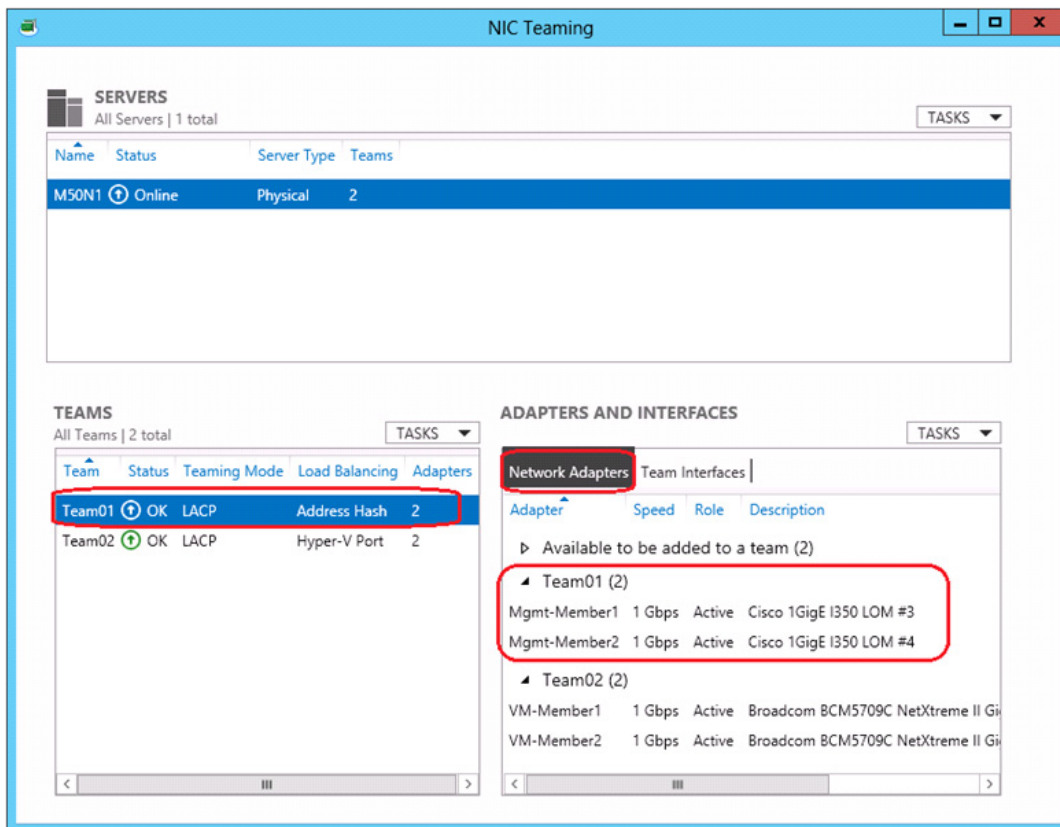
**Figure 48**      **Windows NIC Teaming Logical Representation**

**Table 8**      **Details of NIC Teaming**

Team Name	Team Member	Team Interface Name	VLAN ID
Team01	1. Mgmt Member1	1. Mgmt OS	Default
	2. Mgmt Member 2	2. LM	22
Team02	1. VM-Memeber1	3. CSV	24
	2. VM-Member1	1. VMComm	Default

- a. From the Windows PowerShell prompt create NIC team using the details given in [Table 8](#).

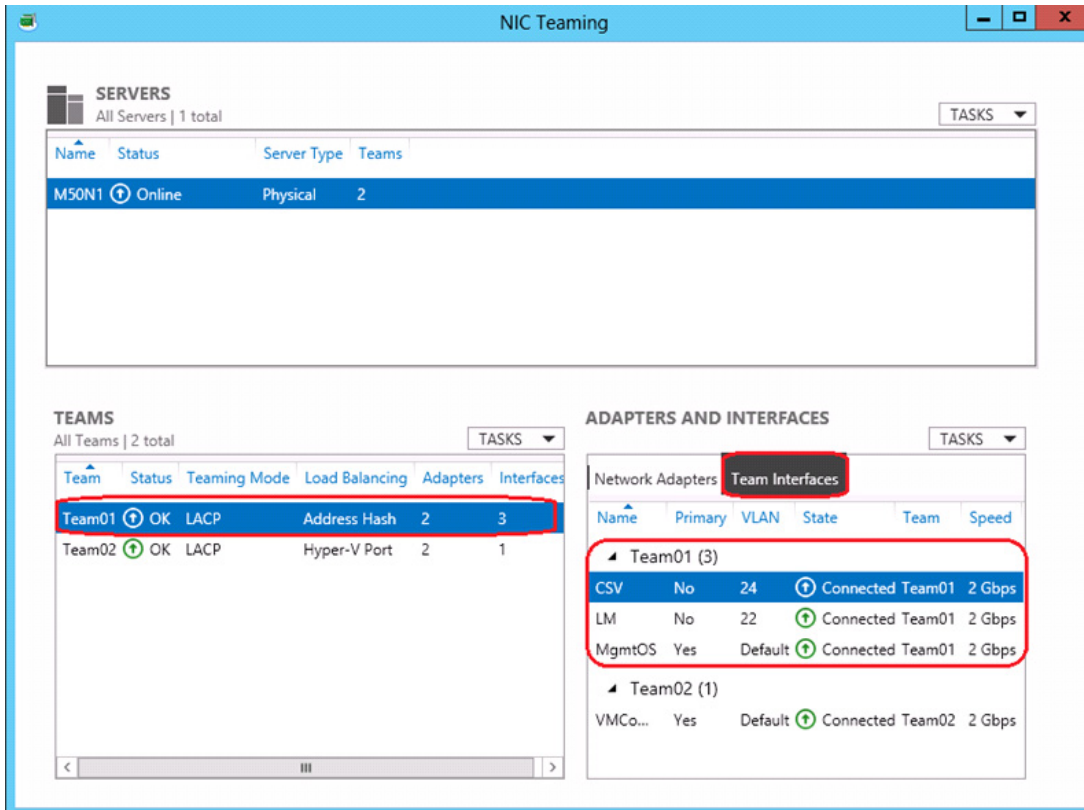
```
New-NetLbfoTeam -Name <Team01> -TeamMembers <Mgmt-Member1,Mgmt-Member2>
-TeamNicName <MgmtOS> -TeamingMode LACP -a
```

**Figure 49**      **NIC Teaming GUI - Team 01 Members**

```
Add-NetLbfoTeamNic -Team <Team01> -VlanID <22> -Name <LM> -a
Add-NetLbfoTeamNic -Team <Team01> -VlanID <24> -Name <CSV> -a
```

- b. Add two team interfaces to the above team for segregating CSV and Live Migration traffic.

Figure 50 Teaming GUI - Team 01 tNICs



- c. Create the second NIC team for the virtual machine traffic.

```
New-NetLbfoTeam -Name <Team02> -TeamMembers <VM-Member1,VM-Member2>
-TeamNicName <VMComm> -TeamingMode LACP -LoadBalancingAlgorithm HyperVPort -a
```

**Figure 51**      **NIC Teaming GUI - Team02 Members**

The screenshot displays the 'NIC Teaming' window. At the top, there's a 'SERVERS' section with a table showing one server, 'M50N1', which is 'Online' and has '2' teams. Below this is the 'TEAMS' section, which shows two teams: 'Team01' and 'Team02'. 'Team02' is selected and highlighted with a red box. It has a status of 'OK', uses 'LACP' for teaming mode, 'Hyper-V Port' for load balancing, and has '2' adapters. To the right of the 'TEAMS' section is the 'ADAPTERS AND INTERFACES' section. It has two tabs: 'Network Adapters' (selected and highlighted with a red box) and 'Team Interfaces'. Under 'Network Adapters', there are two expandable sections: 'Available to be added to a team (2)' and 'Team02 (2)'. The 'Team02 (2)' section is expanded and highlighted with a red box, showing two members: 'VM-Member1' and 'VM-Member2'. Both are '1 Gbps' and 'Active', with a description of 'Broadcom BCM5709C NetXtreme II Gi'.

**SERVERS**  
All Servers | 1 total

Name	Status	Server Type	Teams
M50N1	Online	Physical	2

**TEAMS**  
All Teams | 2 total

Team	Status	Teaming Mode	Load Balancing	Adapters
Team01	OK	LACP	Address Hash	2
Team02	OK	LACP	Hyper-V Port	2

**ADAPTERS AND INTERFACES**

**Network Adapters**

Adapter	Speed	Role	Description
Available to be added to a team (2)			
Team01 (2)			
Team02 (2)			
VM-Member1	1 Gbps	Active	Broadcom BCM5709C NetXtreme II Gi
VM-Member2	1 Gbps	Active	Broadcom BCM5709C NetXtreme II Gi

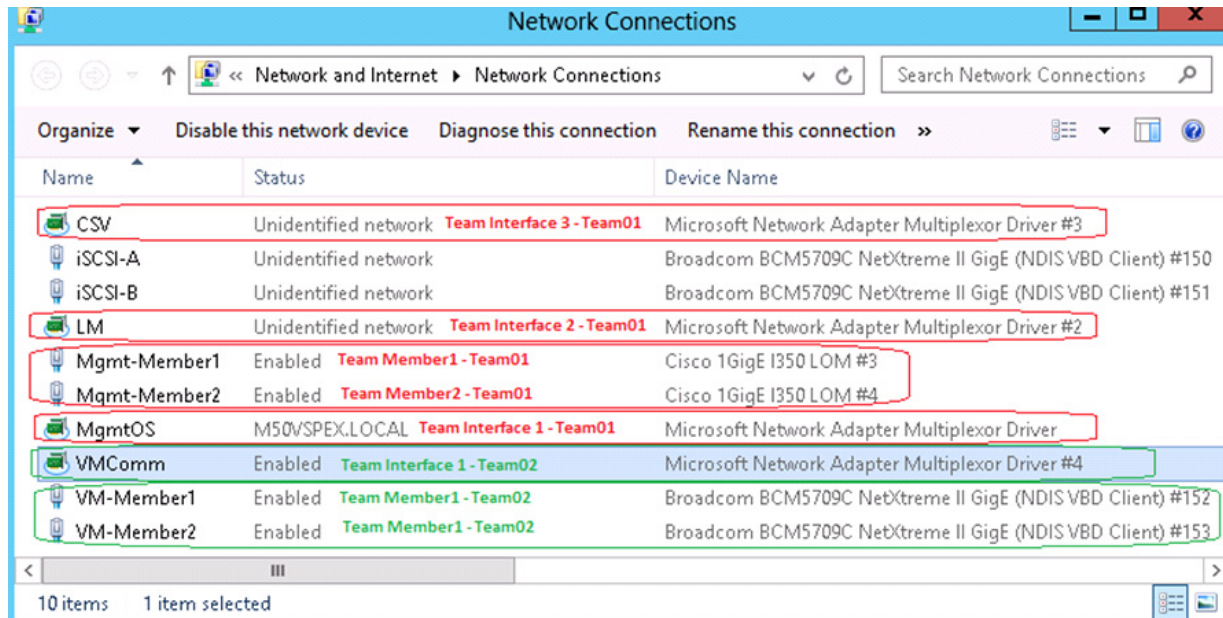
Figure 52 NIC Teaming GUI - Team02 tNICs

The screenshot displays the 'NIC Teaming' window. It is divided into three main sections: 'SERVERS', 'TEAMS', and 'ADAPTERS AND INTERFACES'.

- SERVERS:** Shows a table with one server, 'M50N1', which is 'Online' and has a 'Physical' server type with 2 teams.
- TEAMS:** Shows a table with two teams. 'Team02' is highlighted with a red box. It has a status of 'OK', uses 'LACP' for teaming mode, 'Hyper-V Port' for load balancing, and has 2 adapters and 1 interface.
- ADAPTERS AND INTERFACES:** This section is further divided into 'Network Adapters' and 'Team Interfaces'. The 'Team Interfaces' tab is selected and highlighted with a red box. It shows two teams:
  - Team01 (3):** Contains three interfaces: 'CSV' (No, VLAN 24, Connected to Team01, 2 Gbps), 'LM' (No, VLAN 22, Connected to Team01, 2 Gbps), and 'MgmtOS' (Yes, Default, Connected to Team01, 2 Gbps).
  - Team02 (1):** Contains one interface: 'VMComm' (Yes, Default, Connected to Team02, 2 Gbps). This entire section is highlighted with a red box.

**Note**

NICs used for iSCSI traffic are not teamed. Instead, Microsoft MPIO (Multipath Input/Output) will be used for load balancing and failover.

**Figure 53**      **Network Connections**

Windows Server 2012 NIC Teaming (LBFO) Deployment and Management Guide can be downloaded from the below URL:

<http://www.microsoft.com/en-in/download/details.aspx?id=30160>

- Assign IP addresses to the iSCSI NICs and the team interfaces (except for the VMComm) created in the above steps.

```
New-NetIPAddress -InterfaceAlias <MgmtOS> -IPAddress <10.29.150.92>
-DefaultGateway <10.29.150.1> -PrefixLength <24>
New-NetIPAddress -InterfaceAlias <LM> -IPAddress <10.10.22.21> -PrefixLength <24>
New-NetIPAddress -InterfaceAlias <CSV> -IPAddress <10.10.24.21> -PrefixLength <24>
New-NetIPAddress -InterfaceAlias <iSCSI-A> -IPAddress <10.10.20.21> -PrefixLength <24>
New-NetIPAddress -InterfaceAlias <iSCSI-B> -IPAddress <10.10.21.21> -PrefixLength <24>
```

- Disable DNS registration for all NICs except Management NIC.

```
Set-DnsClient -InterfaceAlias <iSCSI-A,iSCSI-B,CSV,LM> -Register $false
```

- Add the Active Directory DNS server address to the Management NIC.

```
Set-DnsClientServerAddress -InterfaceAlias <MgmtOS> -ServerAddresses
<10.29.150.90>
```

In the above command replace the <MgmtOS> with the name of the NIC used for management traffic and add an IP address of your DNS server next to -ServerAddress.

## Host Rename and Active Directory Domain Join

- Rename the hosts from the PowerShell prompt

```
Rename-Computer -NewName <m50n>1 -restart
```

In the above command replace the <m50n1> with a name per your organization's naming standard.

2. Join the hosts to the Active Directory domain from the PowerShell prompt.

```
Add-Computer -DomainName <m50vspex> -Restart
```

In the above command replace the <m50vspex> with the Active Directory domain name in your network.

## Install Roles and Features

Install Hyper-V, Failover-Clustering, Multipath I/O roles/features and restart the host.

```
Add-WindowsFeature Hyper-V, Failover-Clustering, Multipath-IO  
-IncludeManagementTools -Restart
```

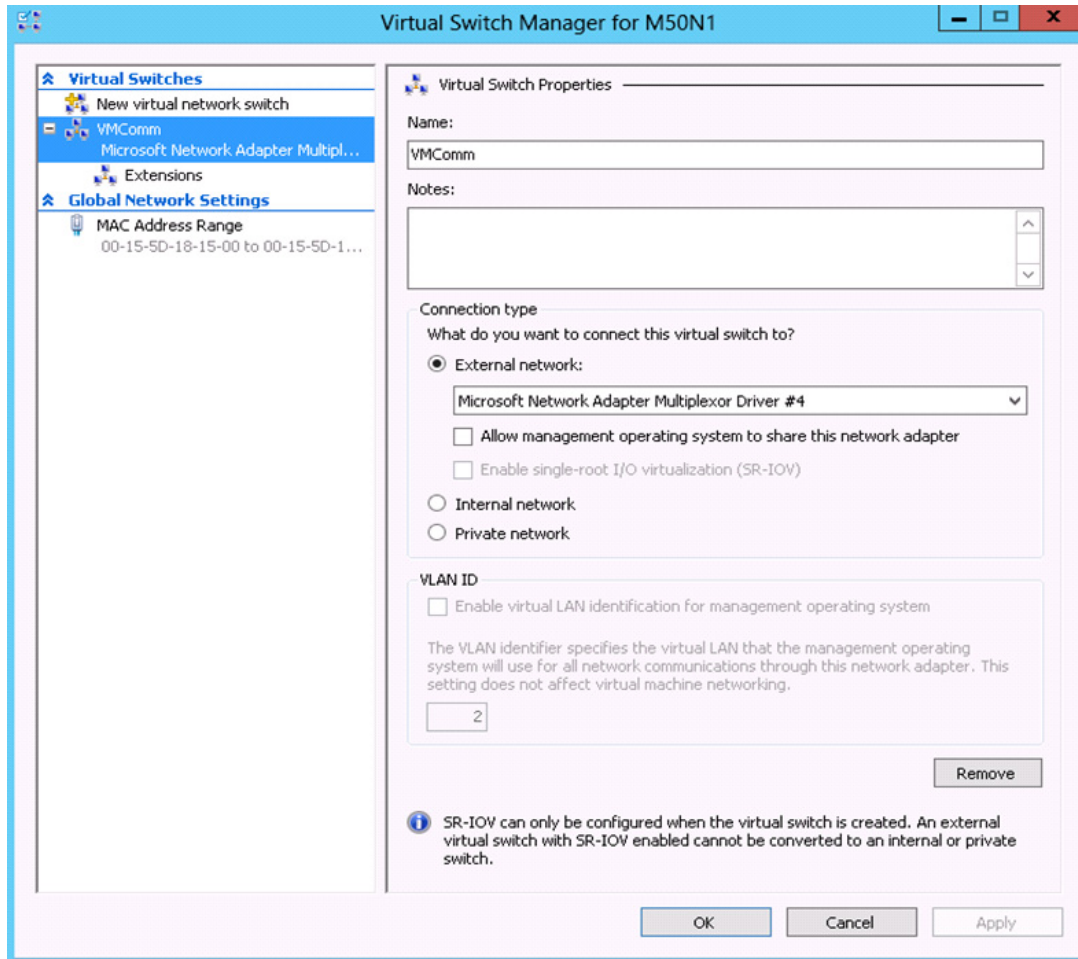
## Configure the Hyper-V Virtual Switch

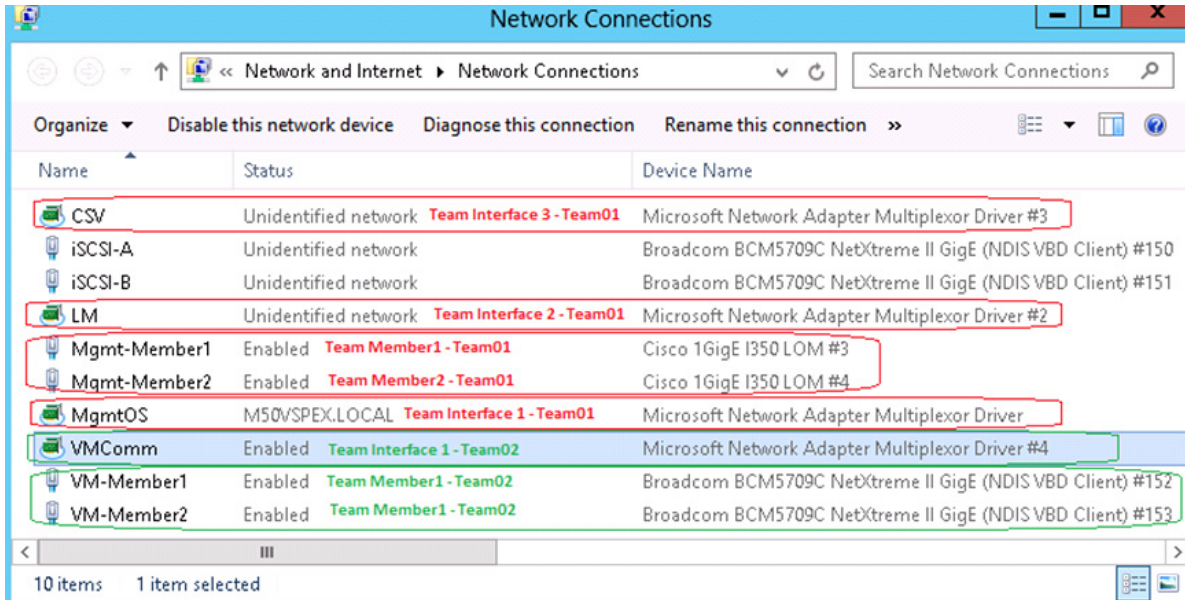
1. Create Hyper-V virtual *switch* using the team interface created above for VM traffic.

```
New-VMSwitch -Name VMComm -NetAdapterName VMComm -AllowManagementOS $false
```

In the above command replace the <VMComm> with the name of your team interface created for VM traffic.



**Figure 54**      **Hyper-V Virtual Switch Manager**

**Figure 55**      **Network Connections**

2. If planning for guest clustering using iSCSI, then create Hyper-V virtual switches for the iSCSI. This step is optional.

```
New-VMSwitch -Name iSCSI-A -NetAdapterName iSCSI-A -AllowManagementOS $true
-EnableIov $true
New-VMSwitch -Name iSCSI-B -NetAdapterName iSCSI-B -AllowManagementOS $true
-EnableIov $true
```

In the above command replace the *<iSCSI-A>* and *<iSCSI-B>* with the name of your network adapter used for iSCSI traffic.

## Modify Windows Server 2012 iSCSI Registry Parameters

The registry settings in [Table 9](#) should be modified on each server running iSCSI to the VNXe. The settings apply for both the native Windows Server 2012 MPIO DSM and PowerPath unless otherwise noted.

1. In Windows, run the regedit.exe command to start the Windows Registry Editor.
2. Navigate to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet.
3. Right click on the key and select **Find**.
4. Search for the registry values in [Table 9](#). The values will be within the following folder.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{\*\*\*}\\*\*\*\Parameters

**Table 9** *iSCSI Registry Settings for VNXe Array*

Registry Value	Instructions
LinkDownTime	Set to 600 (Decimal)
DelayBetweenReconnect	Find the <b>DelayBetweenReconnect</b> value.
PortalretryCount	Set the <b>PortalRetryCount</b> value so that <b>PortalRetryCount*DelayBetweenReconnect=600</b>
MaxRequestHoldTime	Verify the <b>MaxRequestHoldTime</b> value is set to 600 (Decimal)
SrbTimeoutDelta for Powerpath only	Set to 100 (Decimal) for PowerPath only.

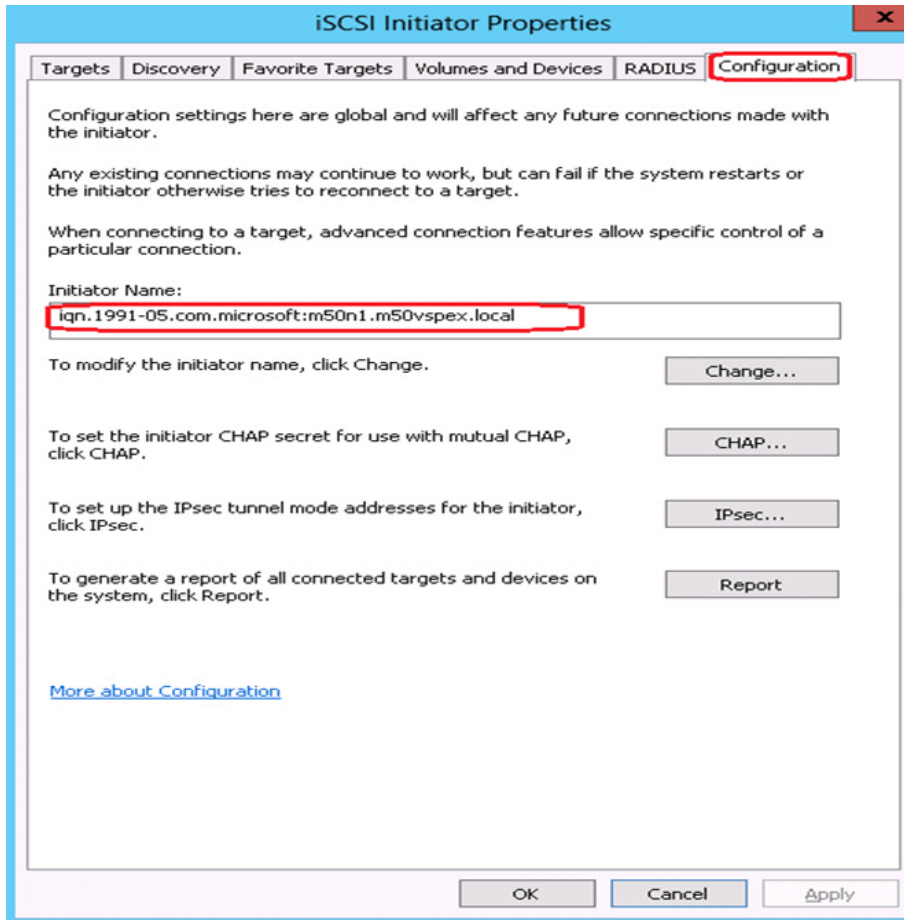
## Enable Host iSCSI Initiator

1. Launch a Windows PowerShell prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.
2. Configure the iSCSI service to start automatically.  

```
Set-Service -Name MSiSCSI -StartupType Automatic
```
3. Start the iSCSI service.  

```
Start-Service -Name MSiSCSI
```
4. Type **iscsicpl.exe** in the PowerShell prompt to open the host iSCSI initiator properties. Note down the initiator name for all the hosts. This is required during the configuration of Storage.

**Figure 56** *iSCSI Initiator Properties - Configuration*



## Prepare the EMC VNXe3150 Storage

This section explains:

- Preparing the storage array
- Aggregate data ports for high-availability
- Create storage pools for Hyper-V datastores
- Create iSCSI server and assign host access privileges

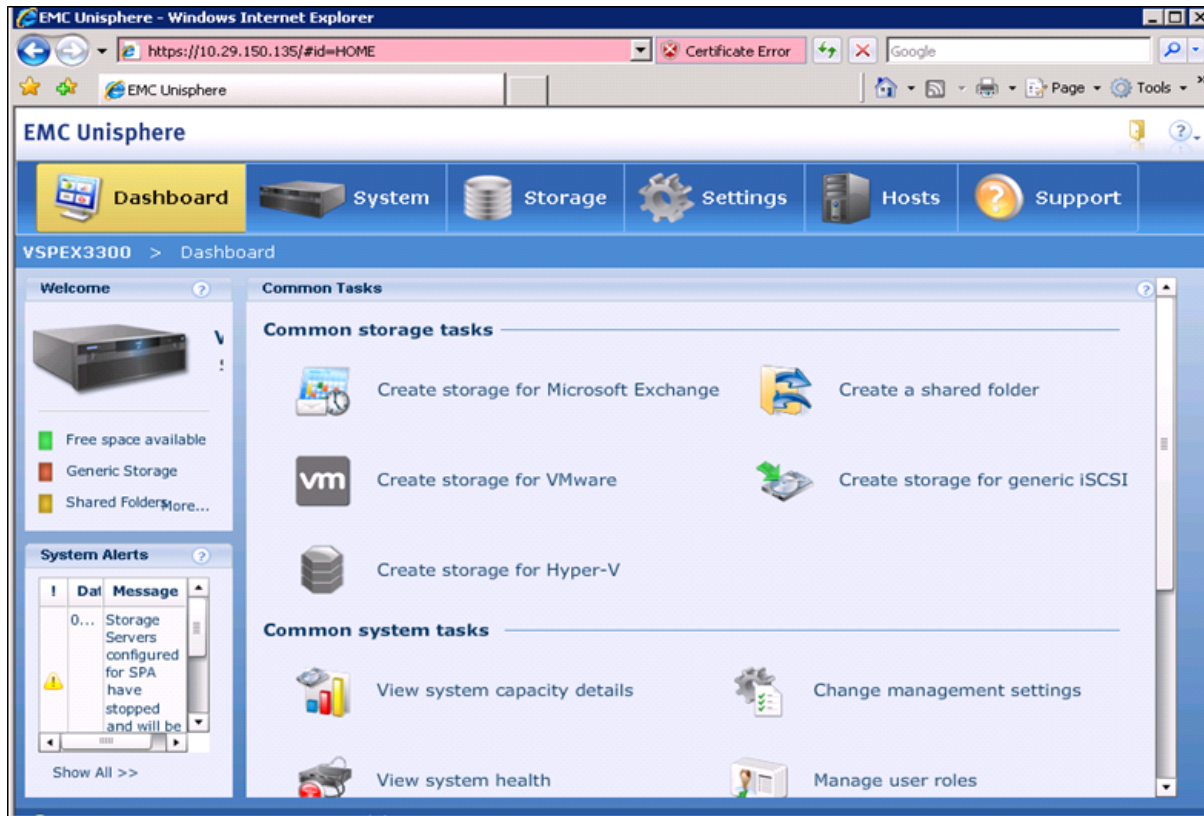
## Initial Setup of VNXe

1. Connect the Ethernet cables from the management and data ports to the network as shown in the cabling guide.
2. Assign an IP address to the management interface or Download and run the Connection Utility to establish an IP address for managing the VNXe storage system. The Connection Utility can be downloaded directly from the product support page.

<http://www.emc.com/support-training/support/emc-powerlink.htm>

3. Connect to the VNXe system from a web browser using the management IP address.

**Figure 57** *EMC Unisphere - Dashboard Page*



**Note**

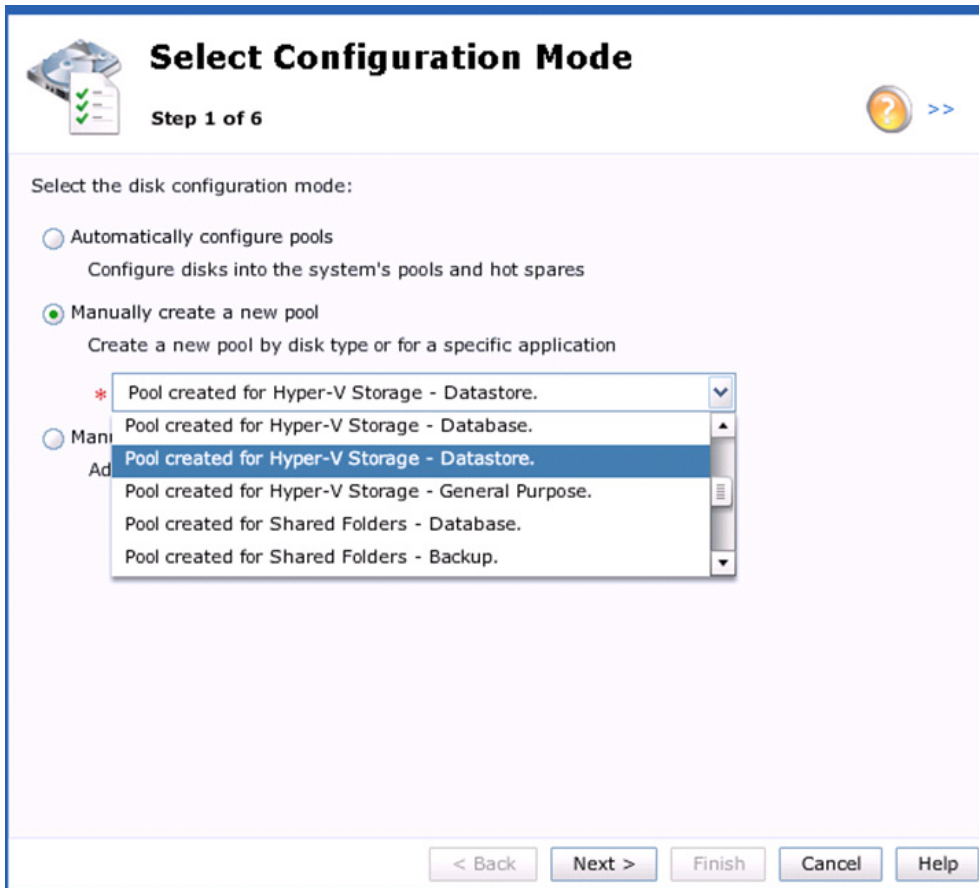
The SP A and SP B network data ports must be connected to the same subnet. In general, both SPs should have mirrored configurations for all front-end cabling (including VLANs) in order to provide Failover.

## Create Storage Pools

Create a pool with the appropriate number of disks as suggested in [Figure 3](#).


1. In Unisphere, choose **System > Storage Pools**.
2. Choose **Configure Disks**.
3. Click the radio button **Manually create a new pool** by Disk Type for SAS drives in the Select Configuration Mode window.

**Figure 58** *EMC Unisphere - Select Mode in Disk Configuration Wizard*



4. Choose the option Pool created for Hyper-V Storage – Datastore from the drop-down list.
5. Specify Pool Name.


**Figure 59** *EMC Unisphere - Specify Pool Name in Disk Configuration Window*



The screenshot shows the 'Specify Pool Name' window in EMC Unisphere. The window has a title bar with a disk icon and a progress indicator showing 'Step 2 of 6'. The main area is light purple and contains the text 'Specify a name and optional description.' Below this, there are two input fields: 'Name: \*' with the value 'VSPEXM50' and 'Description:' with an empty text box. At the bottom, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. A help icon with a question mark and '>>' is located in the top right corner.

6. Select Balanced Perf/Capacity in the Select Storage Type window. The validated configuration uses a single pool with 45 drives.

**Figure 60** *EMC Unisphere - Select Storage Type in Disk Configuration Wizard*



## Select Storage Type

Step 3 of 6


>>

Please select the type of disks you want to use for this new pool.

The disks and their storage types have been rated according to their suitability to the selected application / usage.

Rating	Disk Type	Max Capacity	Storage Profile
☆☆☆	SAS	0 GB (None Available)	Balanced Perf/Capac
☆☆	SAS	0 GB (None Available)	High Performance
☆	EFD	0 GB (None Available)	Best Performance
	NL SAS	0 GB (None Available)	High Capacity

Uses SAS disks to provide a balanced level of storage performance and capacity. This pool type does not offer performance as high as High Performance pools, but it can be adequate for databases with low-to-average performance requirements.

Hyper-V SAS storage pool using RAID 5(6+1).

< Back
Next >
Finish
Cancel
Help

Figure 61 shows the details of the Storage Pool created.



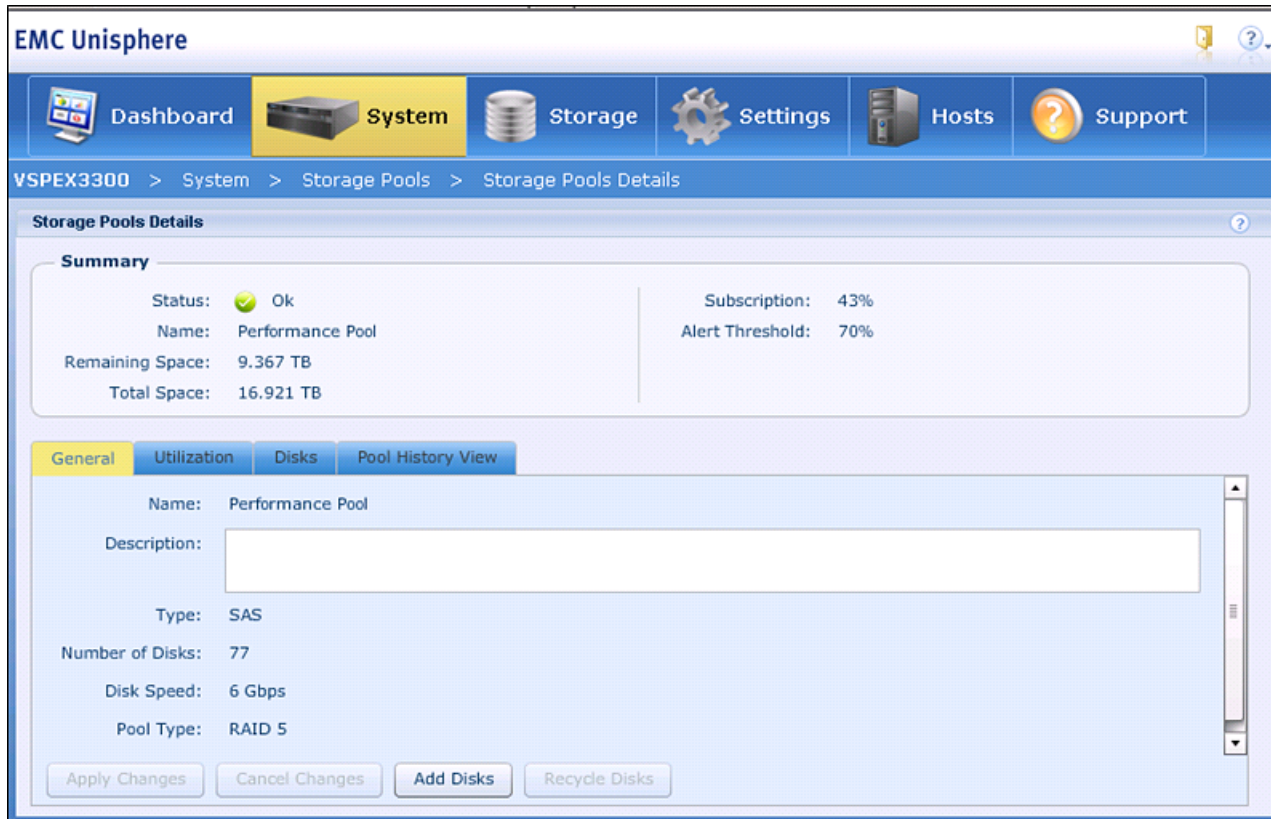
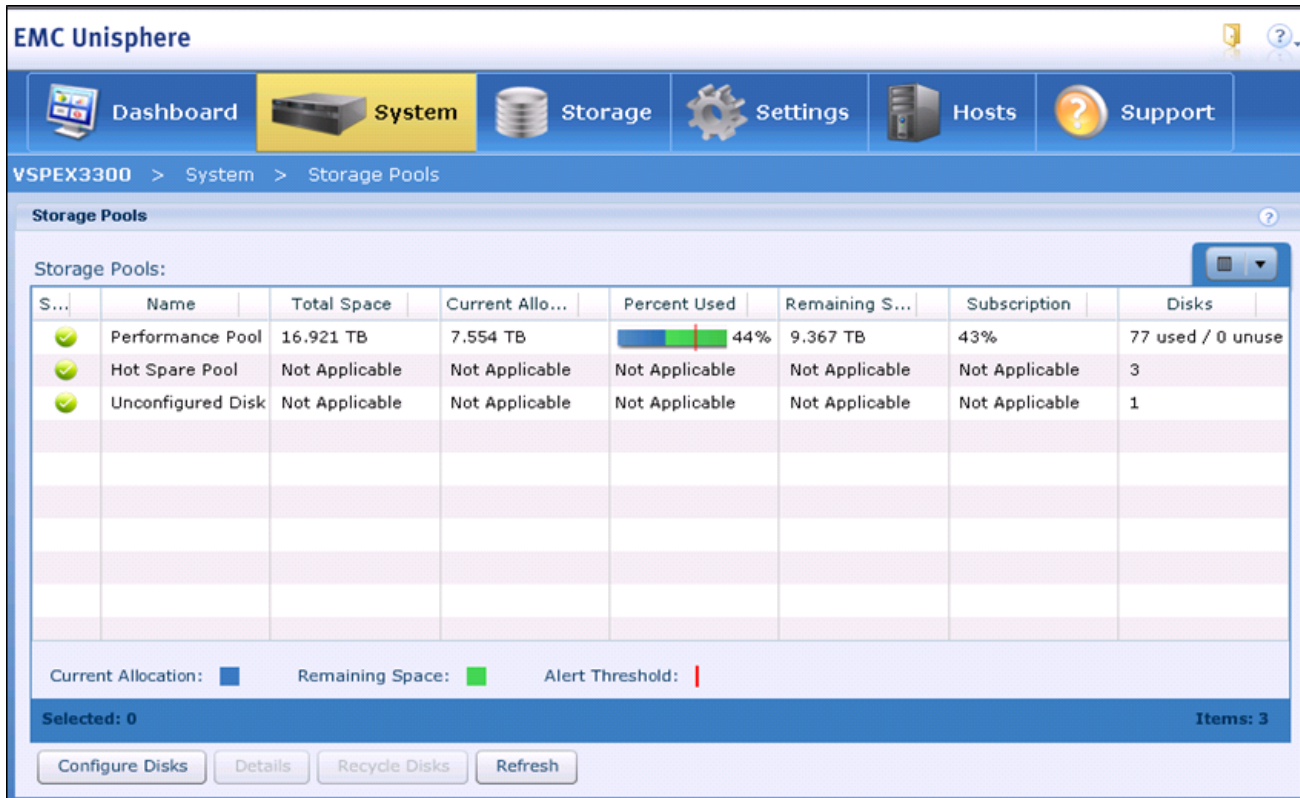
**Figure 61** EMC Unisphere - Storage Pool Details

Figure 62 EMC Unisphere - Storage Pools


**Note**

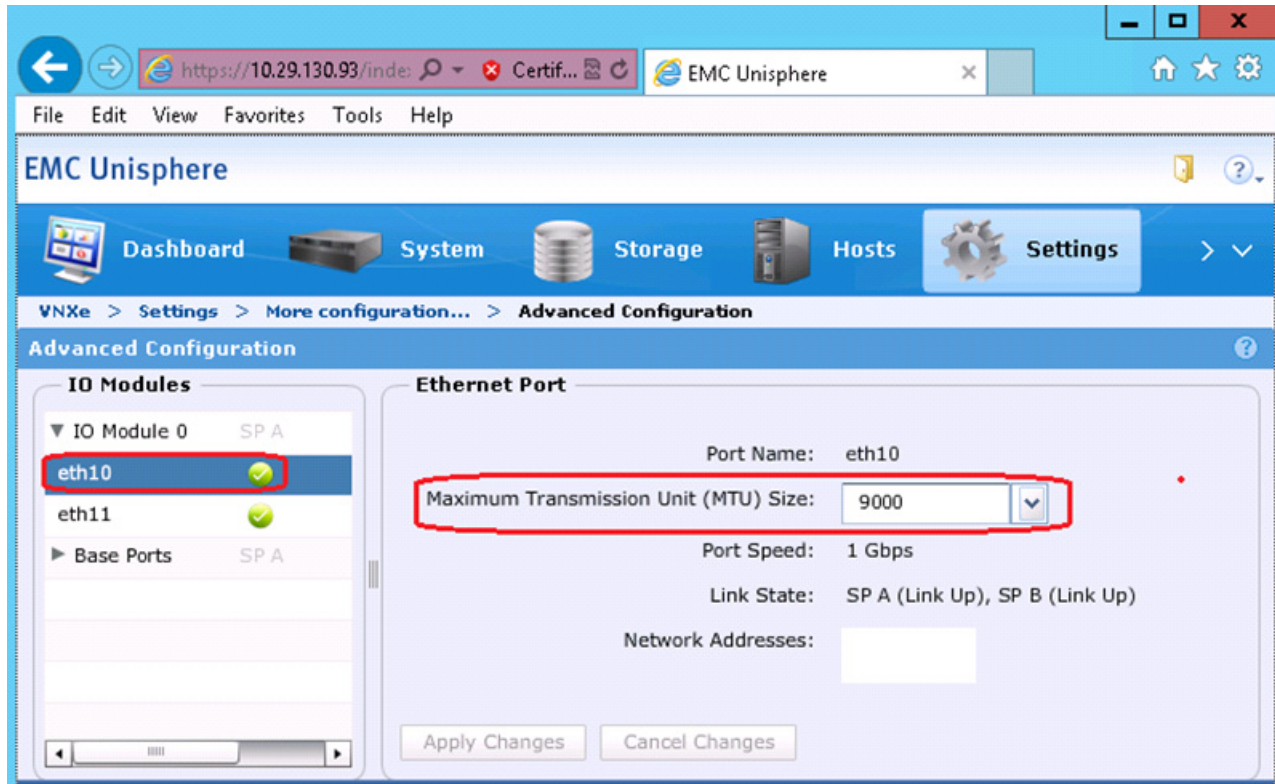
- You should also create your Hot Spare disks at this point.
- As a performance best practice, all of the drives in the pool should be the same size.

## Configure Advanced Features – Jumbo Frames

The Cisco networking environment will have a Maximum Transmission Unit (MTU) size of 9000 for the iSCSI connections to the VNXe. In order to match the configured MTU size via Unisphere, follow these steps:

1. In the EMC Unisphere home page, choose **Settings > More Configuration > Advanced Configuration**.
2. Choose eth10 and set the MTU size to 9000.
3. Choose eth11 and set the MTU size to 9000.

**Figure 63** *EMC Unisphere - Advanced Configuration*



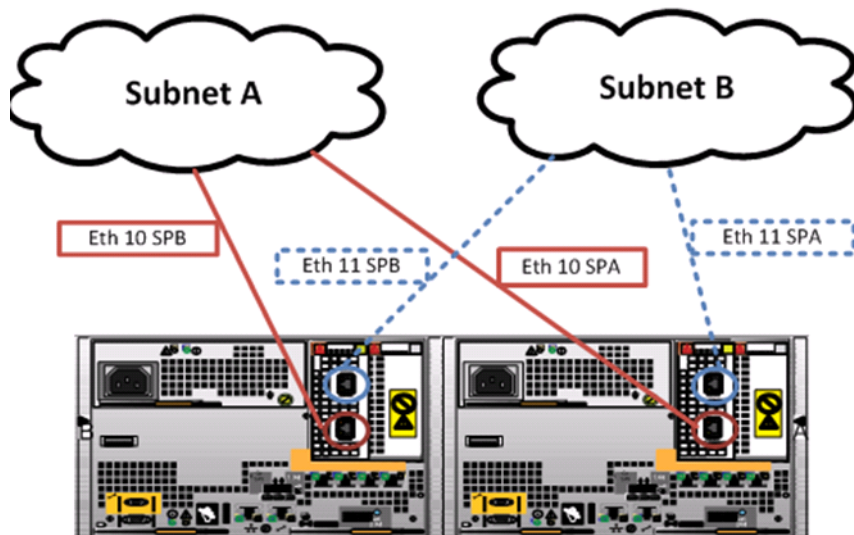
## iSCSI Server Configuration

The iSCSI Storage Server is the portal through which storage will be accessed by the hosts within the Fast Track configuration. The goal of the proposed iSCSI server configuration is to provide redundancy, multi-pathing and balanced access across all 1 GigE connections and both storage processors. Each 1 GigE module will have 2 ports, referred to as eth10 and eth11. Considering there is an I/O module for each service processor, both SPA and SPB will have eth10 and eth11 connections.

iSCSI servers will run on either SPA or SPB. This means storage assigned to a given iSCSI server will only be available to one SP at a given time. To utilize both SPA and SPB concurrently, two iSCSI servers will be created.

With respect to iSCSI server high availability, the eth10 and eth11 connections are paired across the service processors. If an iSCSI server running with an IP address dedicated to eth10 on SP A needs to move to SP B, for maintenance as an example, the IP address will move to the corresponding eth10 port on SPB. Therefore subnet connectivity will need to be the same for the associated eth10 and eth11 connections across the service processors. The [Figure 64](#) shows a logical example of the connections.

**Figure 64** VNXe Array Logical Network Connections



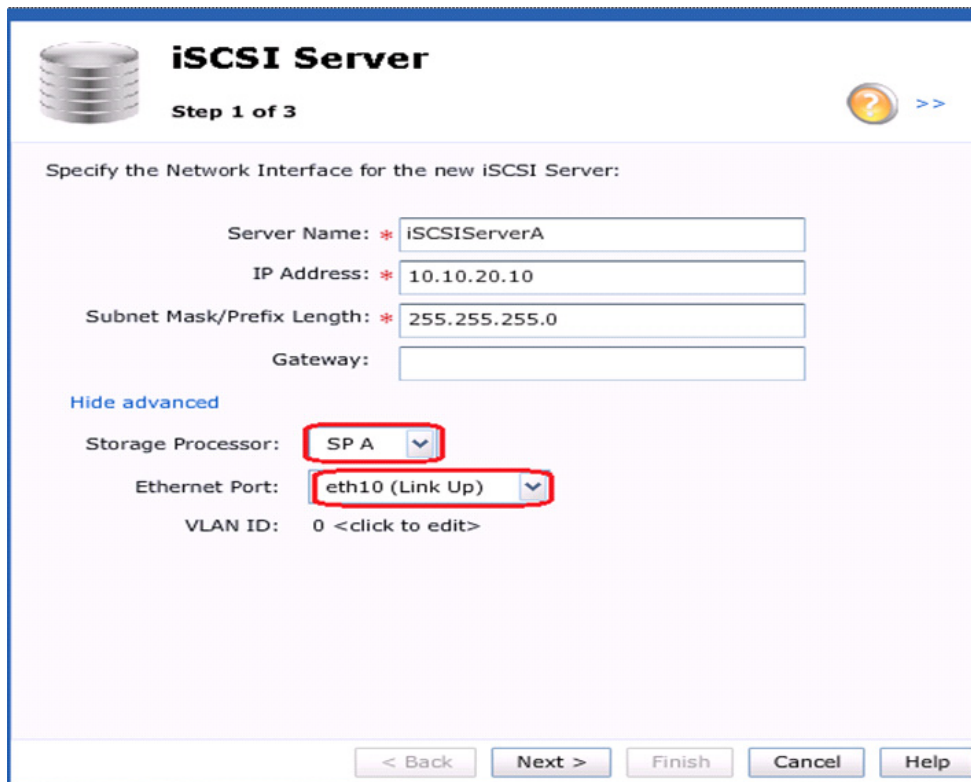
**Table 10** Sample IP Configuration

iSCSI Server A	iSCSI Server B
IP Address Eth10 Subnet A (10.10.20.10/24)	IP Address Eth10 Subnet A (10.10.20.11/24)
IP Address Eth11 Subnet B (10.10.20.10/24)	IP Address Eth11 Subnet B (10.10.21.11/24)

## Configure iSCSI Storage Servers

1. In the ECM Unisphere home page, choose **Settings > iSCSI Server Settings > Add iSCSI Server**.
2. Enter the desired Server Name, IP address, Subnet Mask and Default Gateway (should not need a gateway). Click **Show Advanced** and select the appropriate storage processor (SPA) and Ethernet Port (eth10) as shown in [Figure 65](#).

Figure 65 EMC Unisphere - iSCSI Server SP-A eth10



The image shows a screenshot of the 'iSCSI Server' configuration window in EMC Unisphere. The window is titled 'iSCSI Server' and indicates 'Step 1 of 3'. It prompts the user to 'Specify the Network Interface for the new iSCSI Server:'. The configuration fields are as follows:

- Server Name: \* iSCSIServerA
- IP Address: \* 10.10.20.10
- Subnet Mask/Prefix Length: \* 255.255.255.0
- Gateway: (empty field)
- Hide advanced (link)
- Storage Processor: SP A (dropdown menu)
- Ethernet Port: eth10 (Link Up) (dropdown menu)
- VLAN ID: 0 <click to edit>

At the bottom of the window, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

3. Repeat the steps 1 and 2 to create a second iSCSI server on SP-B and eth10.

Figure 66 EMC Unisphere - iSCSI Server SP-B eth10

**iSCSI Server**  
Step 1 of 3

Specify the Network Interface for the new iSCSI Server:

Server Name: \* iSCSIServerB

IP Address: \* 10.10.20.11

Subnet Mask/Prefix Length: \* 255.255.255.0

Gateway:

Hide advanced

Storage Processor: SP B

Ethernet Port: eth10 (Link Up)

VLAN ID: 0 <click to edit>

< Back Next > Finish Cancel Help

4. Select the previously created iSCSI server and select **Details**.

Figure 67 EMC Unisphere - iSCSI Server Settings

EMC Unisphere

Dashboard System Storage Hosts Settings Support

VNXe > Settings > iSCSI Server Settings

iSCSI Server Settings

iSCSI Servers

Name	IP Addr...	Target	Storage Processor	Ethernet Port	Status
iSCSIServerA	10.10.20.10	iqn.1992-05.com.emc:apm001237028350000-3-vnxe	SP A	eth10, eth11	Ok
iSCSIServerB	10.10.20.11	iqn.1992-05.com.emc:apm001237028350000-8-vnxe	SP B	eth10, eth11	Ok

2 items

Add iSCSI Server Details Remove

5. In the **iSCSI Server Details** window, click **Add Network Interface**.
6. Enter the appropriate IP Address, Subnet Mask and Gateway information.

**Figure 68** *EMC Unisphere - iSCSI Server SP-A eth11*

**Add network interface**

IP Address: \* 10.10.21.10

Subnet Mask/Prefix Length: \* 255.255.255.0

Gateway:

[Hide advanced](#)

Ethernet Port: eth11 (Link Up) ▼

VLAN ID: 0 <click to edit>

Add Cancel

7. Repeat the steps 4,5, and 6 for the iSCSI Server instance assigned to the other storage processor, SP-B.

**Figure 69** *EMC Unisphere - iSCSI Server SP-B eth11*

**Add network interface**

IP Address: \* 10.10.21.11

Subnet Mask/Prefix Length: \* 255.255.255.0

Gateway:

[Hide advanced](#)

Ethernet Port: eth11 (Link Up) ▼

VLAN ID: 0 <click to edit>

Add Cancel



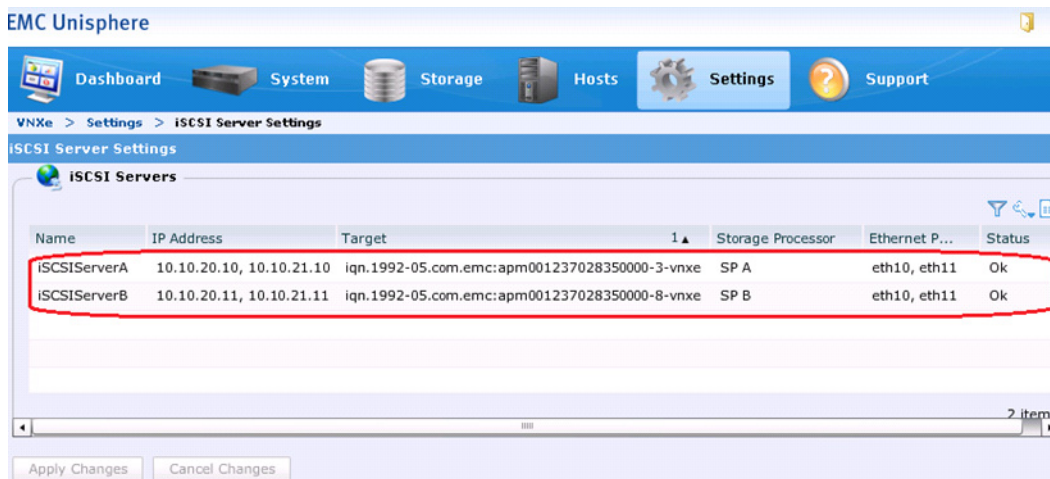


**Note**

In VNXe storage systems, for fail safe networking (FSN) and high availability features to work, the peer ports on both storage processors must belong to the same subnet. For more information about high availability in VNXe storage systems is available in the below URL.

<http://www.emc.com/collateral/hardware/white-papers/h8178-vnxe-storage-systems-wp.pdf>

**Figure 70 EMC Unisphere - iSCSI Server Settings**



## Create Hyper-V Datastores

1. In the EMC Unisphere home page, choose **Storage > Microsoft Hyper-V > Create**.
2. Enter a name and click **Next**.

**Figure 71** *EMC Unisphere - Specify Name in Hyper-V Storage Wizard*

**Specify Name**  
Step 1 of 6

Enter a name for the Hyper-V datastore.

Name: \* M50-WitnessDisk

Description: LUN for Cluster Quorum/Witness Disk

< Back Next > Finish Cancel Help

3. Select the pool and iSCSI server, enter the size 10GB. Do not enable Thin Provisioning and click **Next**.



**Note**

The default size of the Hyper-V datastore is 100 GB. The max size possible is 1.999 TB and the minimum size required is 10 GB.

Figure 72 EMC Unisphere - Configure Storage in Hyper-V Storage Wizard

**Configure Storage**  
Step 2 of 6

Configure the storage for this Hyper-V datastore:  
Select a storage pool with available space on the selected iSCSI server.

Storage Server: iSCSIServerA (SP A) [More information...](#)

Type	1 ▲	Pool	Available	Percent Used	Subscription
SAS		Performance Pool	10.672 TB	35%	13%

Percent Available:  Percent Used:  Alert Threshold:

Size: \*  GB

☐ Thin

< Back Next > Finish Cancel Help

- Click the radio button **Do not configure protection storage for this storage resource** for configure protection. If you need additional protection, then additional storage would be required. Please refer to the EMC VNXe storage configuration guide for more details

**Figure 73** EMC Unisphere - Configure Protection in Hyper-V Storage Wizard

**Configure Protection**  
Step 3 of 6

Configure protection storage for replication and snapshots:

- ☒ **Do not configure protection storage for this storage resource.**  
Replication and snapshots can be supported by allocating protection space at a later time.
- ☐ **Configure protection storage, do not configure a snapshot protection schedule.**  
An automated snapshot protection schedule may be configured at a later time.
- ☐ **Configure protection storage, protect data using snapshot schedule:** Default Protection ▼  
This schedule will create snapshots  
Every day at 01:00, keep for 2 days

Note: Times are displayed in Local Time (UTC-0700) in 24-hour format

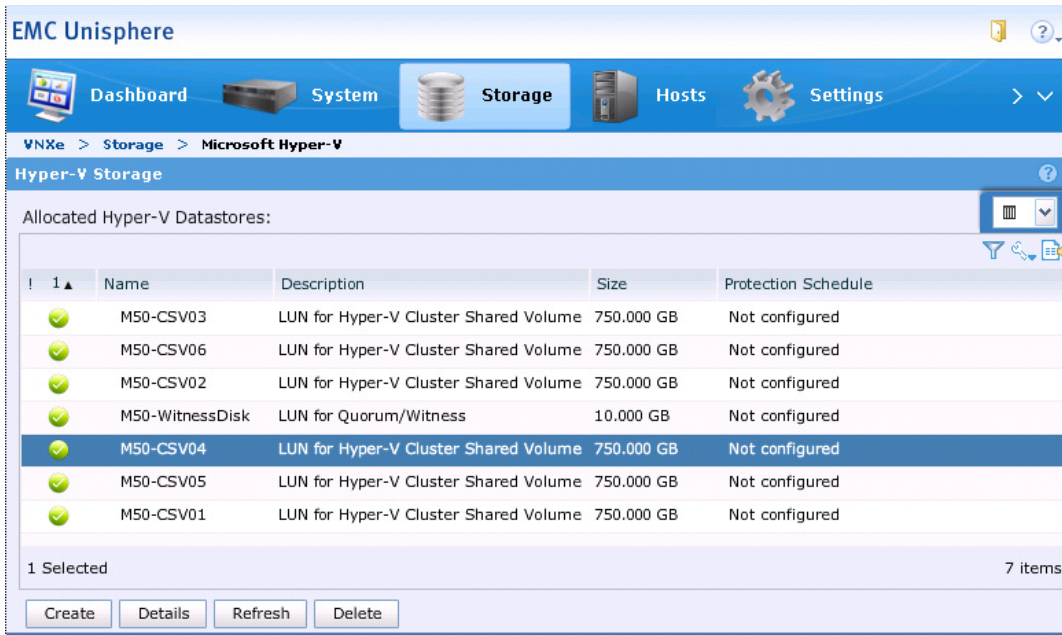
< Back   Next >   Finish   Cancel   Help

5. Click **Next** in Configure Host Access as no host are connected now. Configure Host Access will be completed in VNXe3150 Deployment Procedure – Part 2 in the later section.
6. Repeat the above steps and create 6 Hyper-V datastores for Cluster Shared Volumes of 750GB size.



**Note** 750 GB size Hyper-V datastore for CSV is a suggestion. You can create bigger size datastores.

**Figure 74** *Hyper-V Datastores on VNXe3150 for Cluster Shared Volume*



## Create Hosts and Provide Host Access

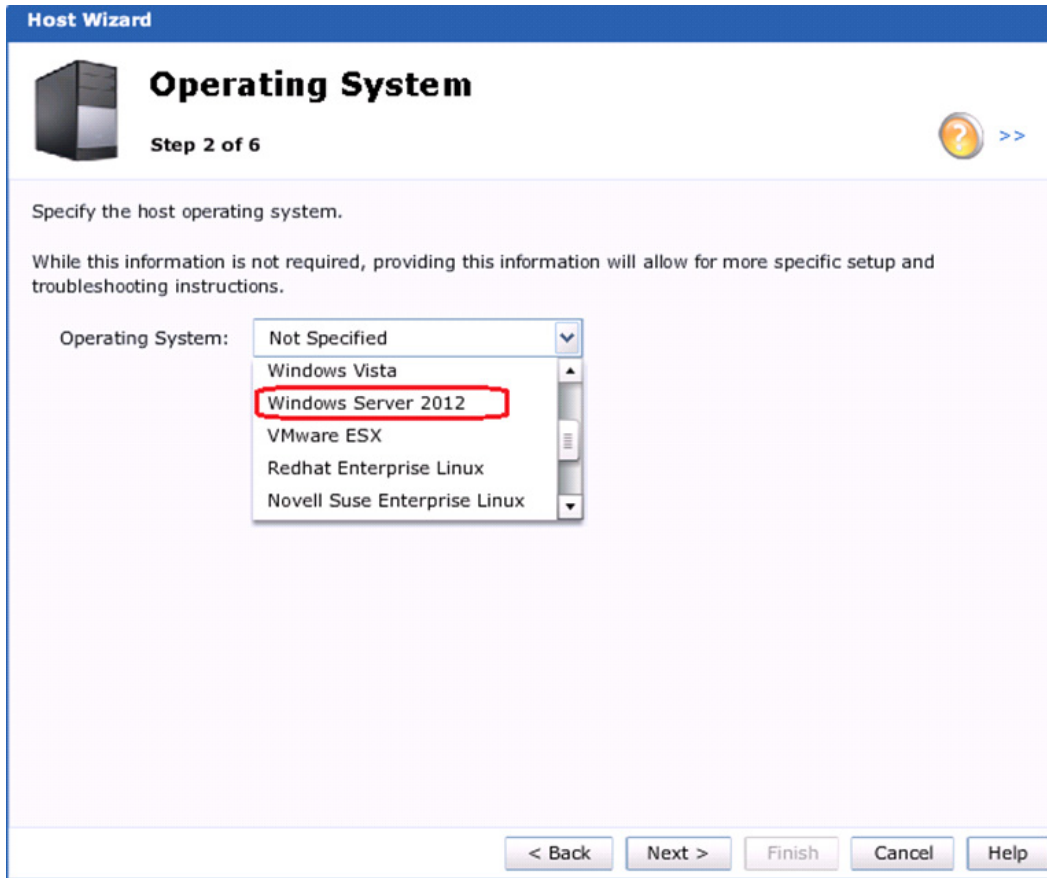
1. In EMC Unisphere, click the **Hosts** tab, and then click **Create Host**.
2. The Create Host window appears. In the Name and Description fields, type the name and description of the new host. Click **Next**.

**Figure 75**      **Specify Name in the VNXe Host Wizard**

The screenshot shows a window titled "Host Wizard" with a sub-header "Specify Name". Below the sub-header, it says "Step 1 of 6". There is a server icon on the left and a help icon with a double arrow on the right. The main area contains the instruction "Enter a name and optional description for the host configuration:". Below this, there are two input fields: "Name: \* M50N1" and "Description: Windows 2012 Hyper-v Cluster Node 1". At the bottom, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

3. The Operating System page appears. Select the host OS from the Operating System list box. Click **Next**.

**Figure 76**      *Operating System Page in VNXe Host Wizard*



4. The Network Address page appears. Select Network Name or IP Address to enter the details of the host.



**Figure 77**      **Network Address Page in VNXe Host Wizard**

**Host Wizard**

## Network Address

Step 3 of 6

Specify the host network address.

You can specify the network address of the host as either a network name or IP Address.

Network Address: ☒ Network Name:

☐ IP Address:  .  .  .

Advanced Storage Access (ASA): ☐ Allow Access

System-wide ASA: Disabled

This setting is only effective if ASA is set to "Enable access on a per-host basis".

[More information...](#)

< Back   Next >   Finish   Cancel   Help

5. The iSCSI Access page appears. Enter the IQN of the Hyper-V host in the IQN field. Host IQN can be found in the iSCSI initiator's configuration tab. Enter the CHAP Secret password if required in your environment.

**Figure 78** *iSCSI Access Page in VNXe Host Wizard*

**Host Wizard**

**iSCSI Access**

Step 4 of 6

If this host is connected to iSCSI storage, you must specify a valid iSCSI address (IQN).

IQN:  [Remove IQN](#)

CHAP Secret:

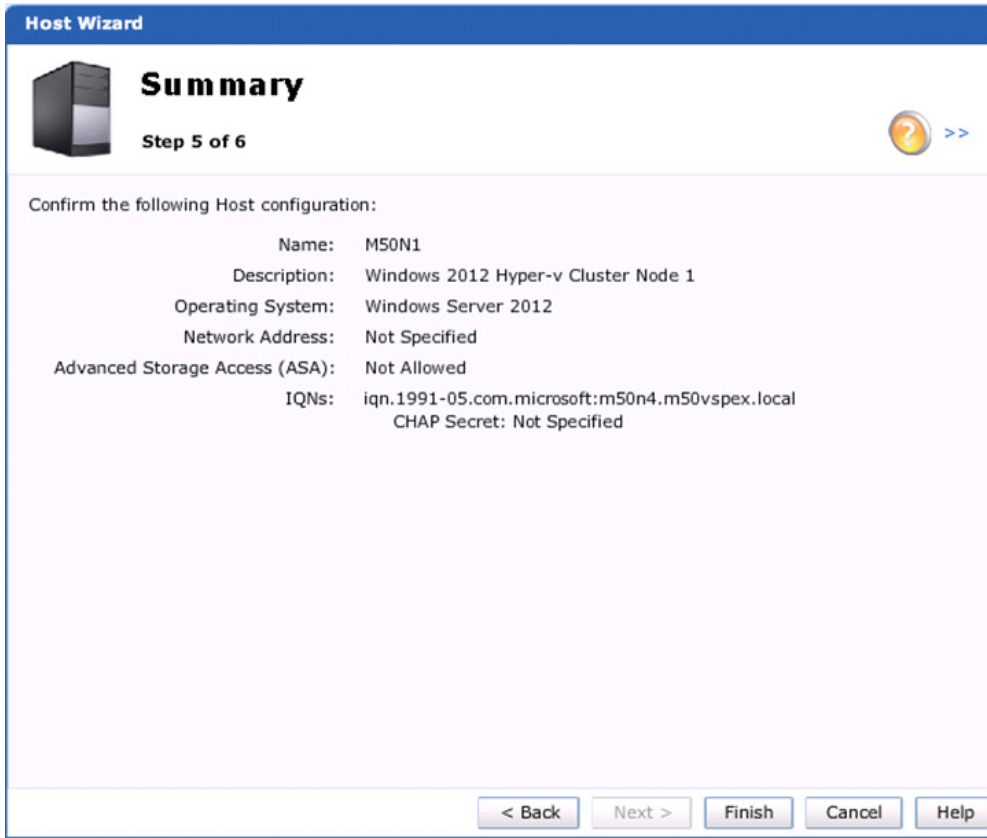
Confirm CHAP Secret:

[Add Another IQN](#)

< Back   Next >   Finish   Cancel   Help

6. The Summary page appears. Review the host details and click **Finish**.

**Figure 79** Summary Page in VNXe Host Wizard



**Host Wizard**

**Summary**

Step 5 of 6

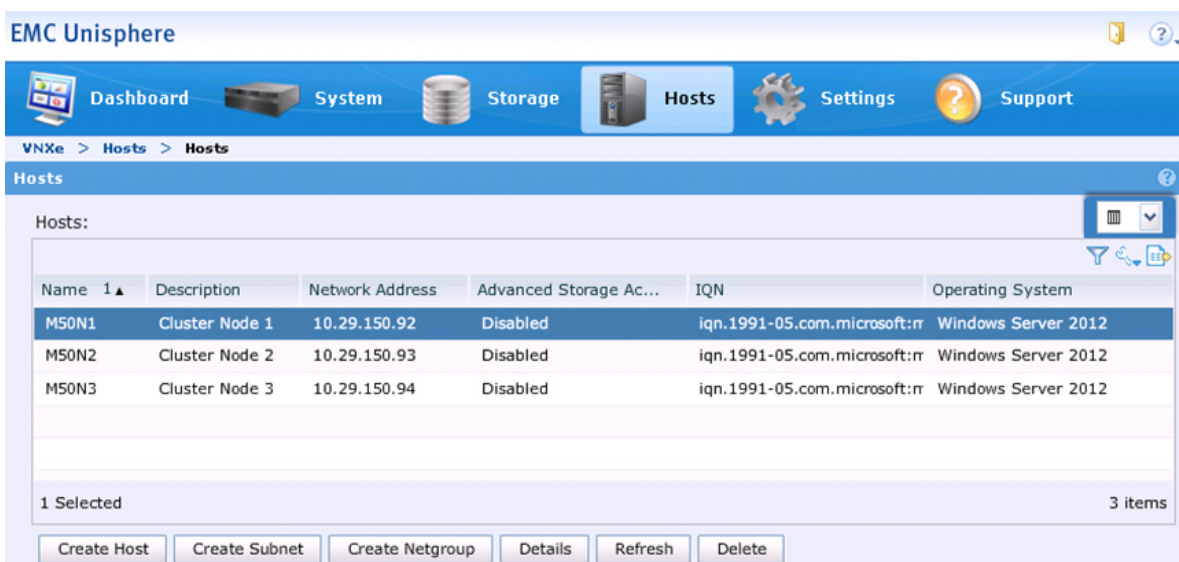
Confirm the following Host configuration:

Name: M50N1  
 Description: Windows 2012 Hyper-v Cluster Node 1  
 Operating System: Windows Server 2012  
 Network Address: Not Specified  
 Advanced Storage Access (ASA): Not Allowed  
 IQNs: iqn.1991-05.com.microsoft:m50n4.m50vspex.local  
 CHAP Secret: Not Specified

< Back   Next >   Finish   Cancel   Help

- Repeat the above steps to create Host list for all Hyper-V hosts.

**Figure 80** VNXe Hosts Page



EMC Unisphere

Dashboard   System   Storage   **Hosts**   Settings   Support

VNXe > Hosts > Hosts

**Hosts**

Hosts:

Name	Description	Network Address	Advanced Storage Ac...	IQN	Operating System
M50N1	Cluster Node 1	10.29.150.92	Disabled	iqn.1991-05.com.microsoft:r	Windows Server 2012
M50N2	Cluster Node 2	10.29.150.93	Disabled	iqn.1991-05.com.microsoft:r	Windows Server 2012
M50N3	Cluster Node 3	10.29.150.94	Disabled	iqn.1991-05.com.microsoft:r	Windows Server 2012

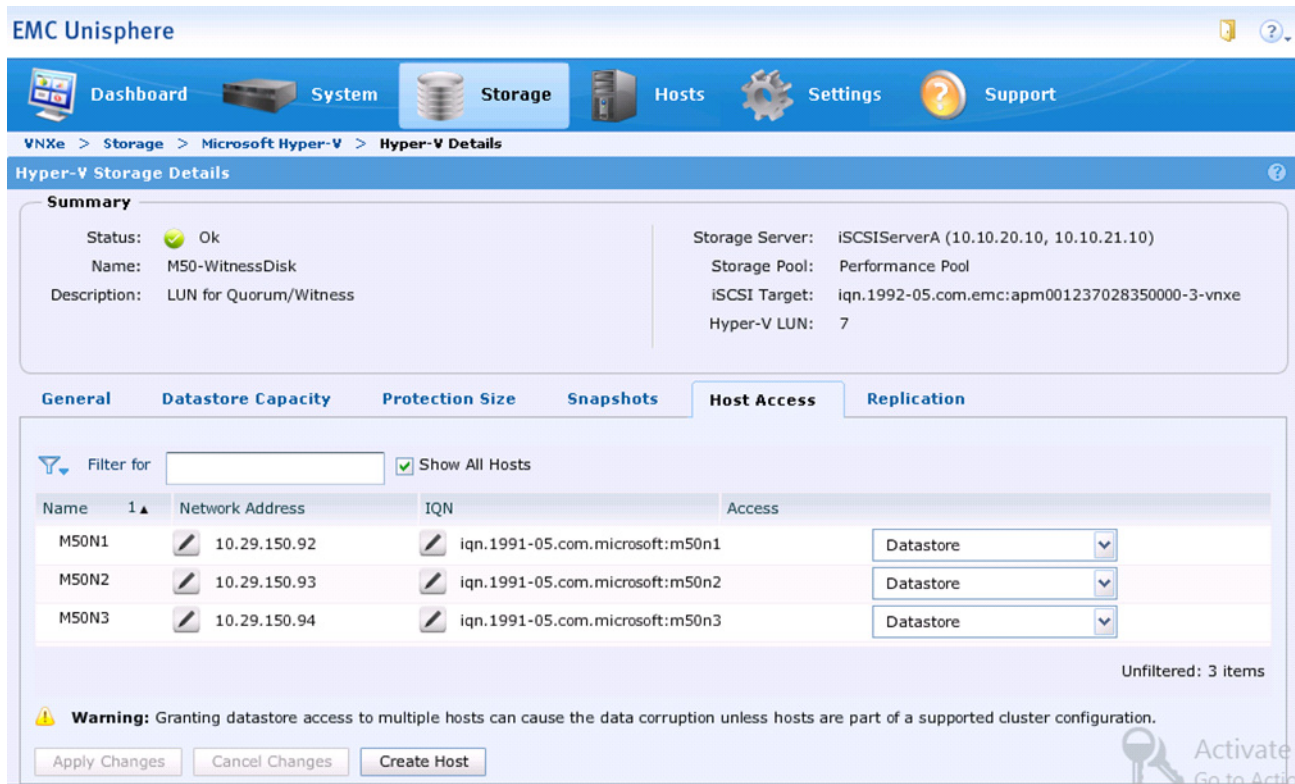
1 Selected   3 items

Create Host   Create Subnet   Create Netgroup   Details   Refresh   Delete

- Click **Storage > Microsoft Hyper-V**. Select an Allocated Datastore and click **Details**.

- Click the **Host Access** tab and from the drop-down list under the Access column select Datastore for all the hosts participating in a Windows Hyper-V cluster.

**Figure 81** VNxe Hyper-V Datastore Details



- Repeat the above steps to provide Host Access for all the Hyper-V datastores created earlier.

## Microsoft Windows Failover Cluster Setup

### Configure MPIO on Windows Server 2012

- Launch a Windows PowerShell prompt by right-clicking the PowerShell icon in the taskbar and selecting Run as Administrator.
- Configure MPIO to claim any iSCSI device.  

```
Enable-MSDSMAutomaticClaim -BusType iSCSI
```
- Set the default load balance policy of all newly claimed devices to round robin.  

```
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```
- Add the following entry to the MPIO device list to register the VNxe Hyper-V disks (datastores) as MPIO devices and set up MPIO to discover iSCSI devices.  

```
New-MSDSMSupportedHW -Vendor "EMC" -ProductId "Celerra"
```



**Note** Ensure there are 5 spaces after EMC and 9 spaces after Celerra

5. Restart the host.

`Restart-Computer`

## Configure iSCSI Initiator

Following steps will show how to configure the iSCSI connections to the VNxe via the iSCSI Initiator Properties GUI. The appendix also includes a PowerShell script that can be used to accomplish the same task.

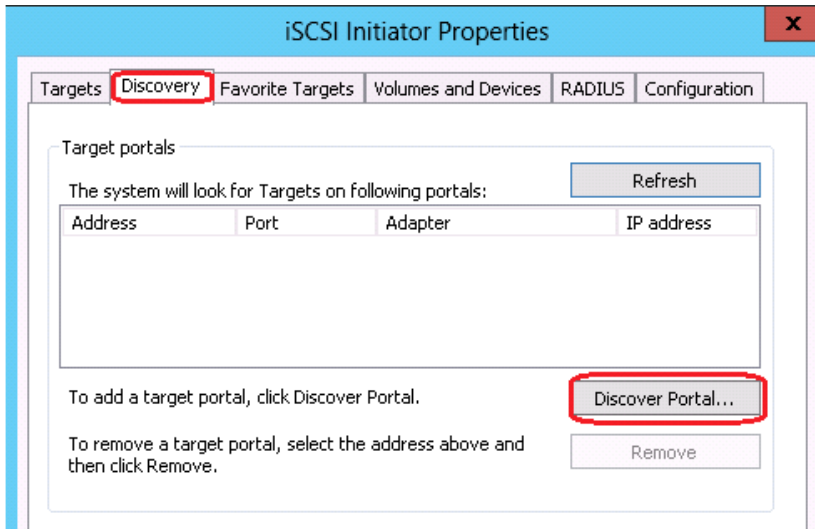
This section describes the steps to configure the host iSCSI initiator to connect to the targets. The host will look for targets on the following portals:

**Table 11** *Example Host iSCSI Initiator and Target Portals Mapping*

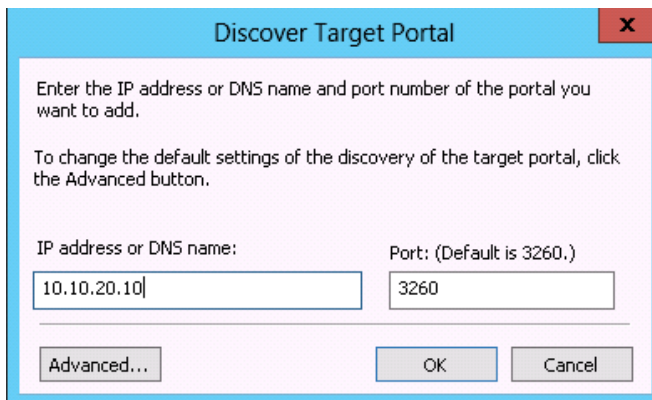
Target Portal IP	Storage Processor Port	Initiator Portal IP	Host iSCSI NIC	Adapter
10.10.20.10	VNxe SP-A eth10 iSCSIServerA	10.10.20.x	iSCSI-A	MS iSCSI Initiator
10.10.21.10	VNxe SP-A eth11 iSCSIServerA	10.10.21.x	iSCSI-B	MS iSCSI Initiator
10.10.20.11	VNxe SP-B eth10 iSCSIServerB	10.10.20.x	iSCSI-A	MS iSCSI Initiator
10.10.21.11	VNxe SP-B eth11 iSCSIServerB	10.10.21.x	iSCSI-B	MS iSCSI Initiator

Follow these steps on all the hosts to connect to iSCSI targets and configure advanced settings:

1. Login to the Windows Server 2012 Hyper-V host.
2. In the Server Manager, click **Local Server** > **Tools** > **iSCSI initiator**
3. In the iSCSI Initiator Properties dialog box, click the **Discovery** tab and then click **Discover Portal**.

**Figure 82** *iSCSI Initiator properties - Discovery*

4. In the IP address or DNS name field, type the IP address of VNXe SP-A eth10 as shown in [Figure 82](#).

**Figure 83** *Discover Target Portal in iSCSI Initiator Properties*

5. The Advanced Settings dialog box appears. Follow these steps:
  - a. Choose Microsoft iSCSI Initiator from the **Local Adapter** drop-down list.
  - b. Choose the IP address of the iSCSI-A NIC from the **Initiator IP** drop-down list.
  - c. If you are required to use the **CHAP**, enter the details else, ignore and click **Ok**.

**Figure 84** *iSCSI Initiator Properties - Advanced Properties*

**Advanced Settings** [?] [X]

**General** | IPsec

**Connect using**

Local adapter: Microsoft iSCSI Initiator

Initiator IP: 10.10.20.21

Target portal IP:

**CRC / Checksum**

☐ Data digest ☐ Header digest

☐ Enable CHAP log on

**CHAP Log on information**

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:m50n1.m50vspex.local

Target secret:

☐ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

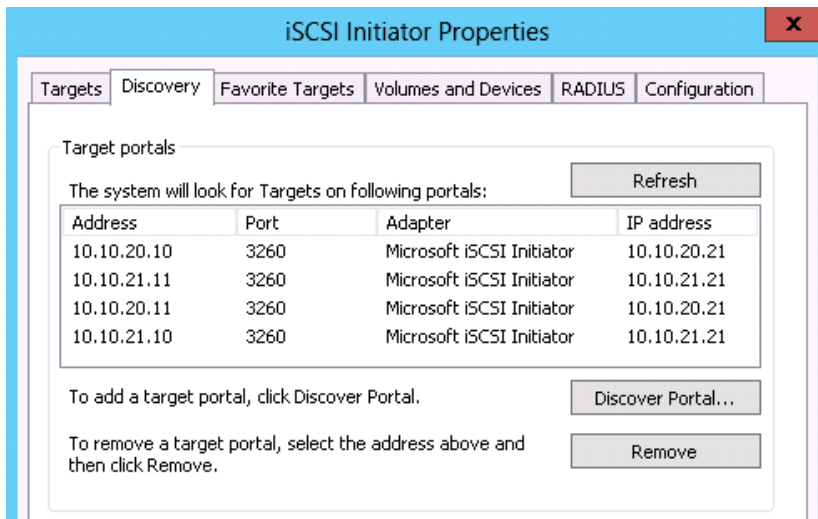
☐ Use RADIUS to generate user authentication credentials

☐ Use RADIUS to authenticate target credentials

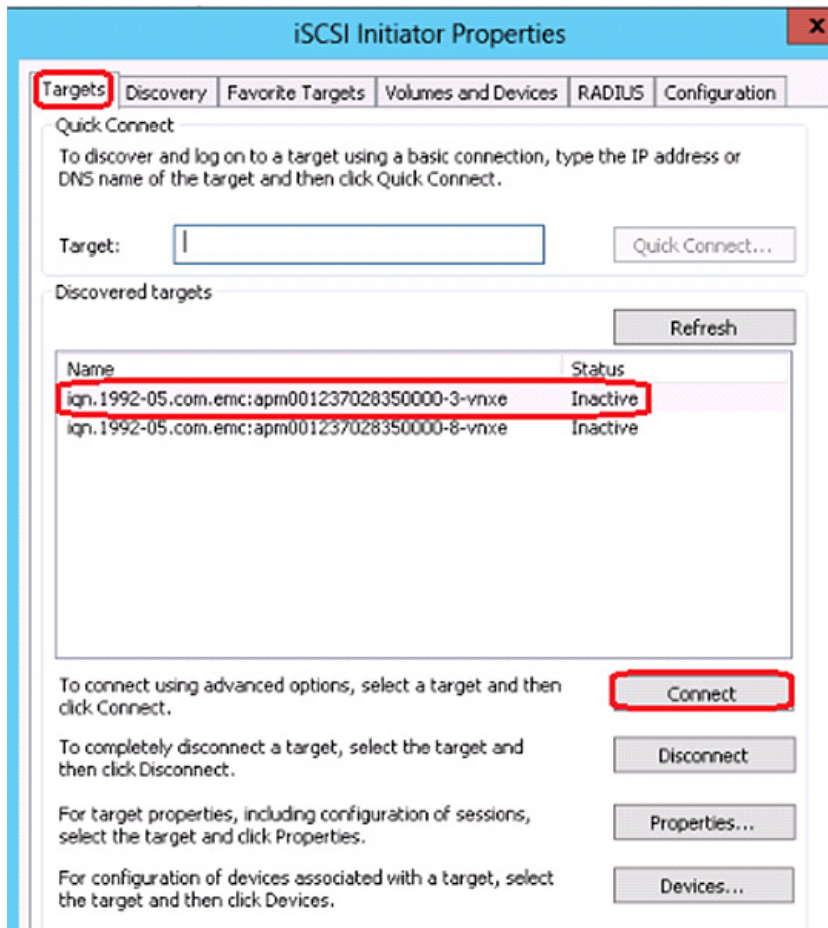
OK Cancel Apply

6. In the iSCSI Initiator Properties dialog box, verify the Target Portals details displayed on the Discovery tab.
7. Repeat the steps from 3 to 6 to add the remaining target portals as specified in [Table 11](#). Once all the target portals are added, the Discover tab will look like as shown in [Figure 82](#).

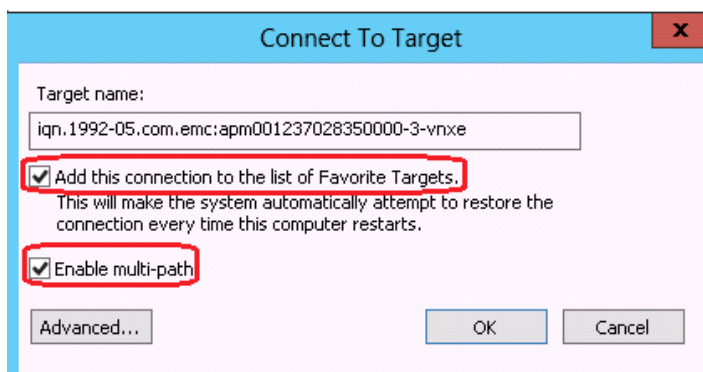


**Figure 85** *iSCSI Initiator Properties - Discovery*

8. Click the **Targets** tab, and then select the first inactive VNXe target name. Click **Connect**.

**Figure 86** *iSCSI Initiator Properties -Targets*

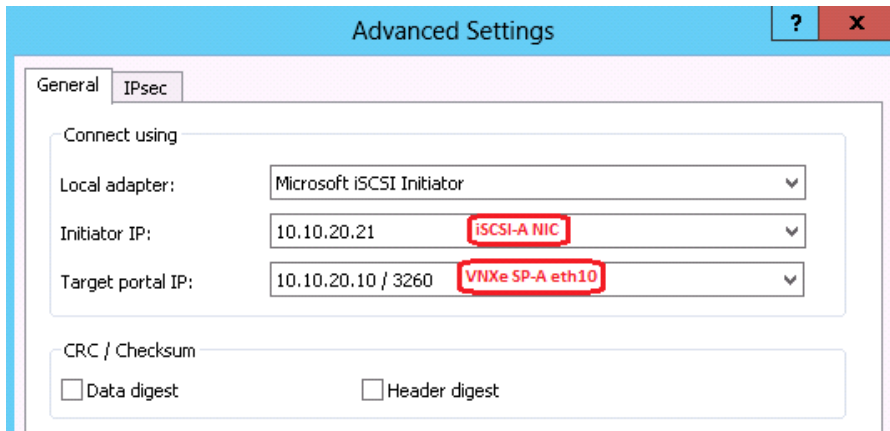
9. The Connect To Target dialog box appears. Follow these steps:
  - a. Select Add this connection to the list of Favorite Targets.
  - b. Select Enable multi path and click **Advanced**.

**Figure 87** *iSCSI Initiator properties - Favorite Targets*

- c. Select the IP address of the iSCSI-A for **Initiator IP** from the drop-down list.

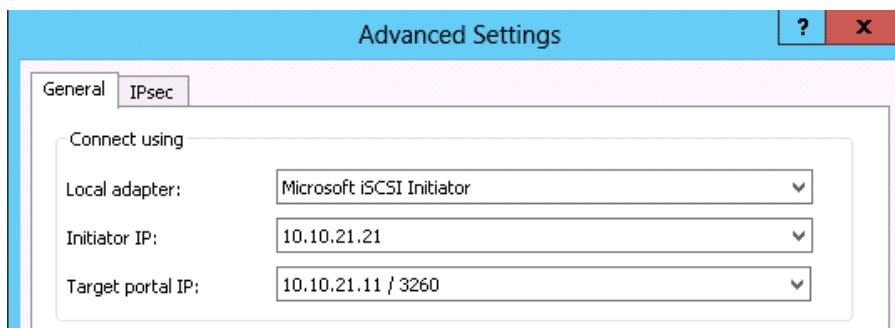
- d. Select the IP address of iSCSI ServerA (VNXe SP-A eth10) for **Target Portal IP** from the drop-down list.

**Figure 88** *iSCSI Initiator Properties - Advanced Settings*

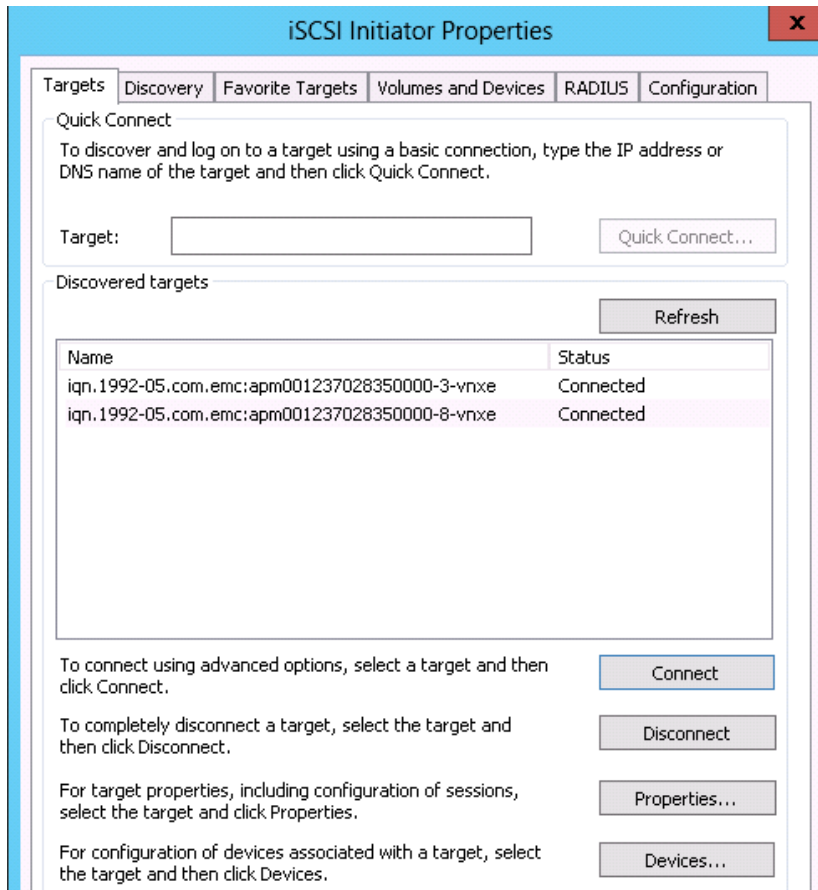
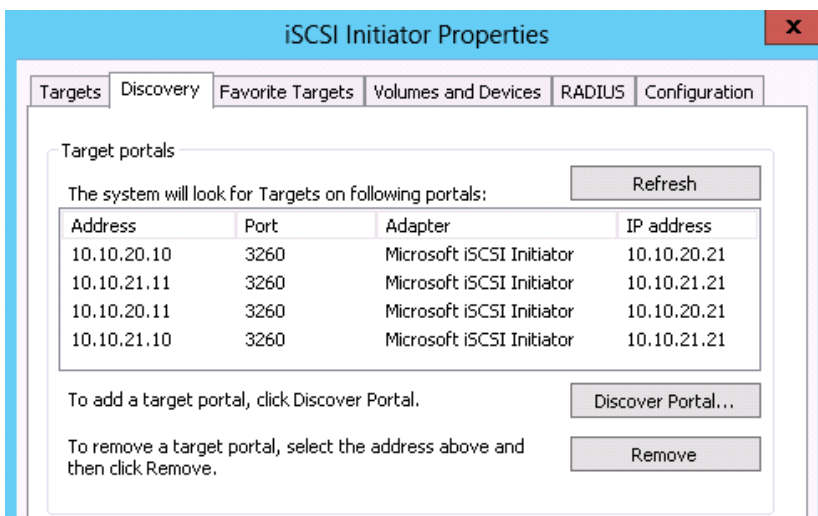


10. Click **Ok** and **OK** to return to the **Targets** tab
11. Repeat the steps 8 to 10 using the IP address of iSCSI ServerB (VNXe SP-B eth11) and host iSCSI-B NIC as shown in [Figure 89](#).

**Figure 89** *iSCSI Initiator Properties - Advanced Settings*



12. Now select the second inactive target and repeat the steps 8 to 11. After this step you should see both the targets showing connected as shown in [Figure 90](#).

**Figure 90** *iSCSI Initiator Properties - Discovered Targets***Figure 91** *iSCSI Initiator Properties - Discovery*

13. When completed, type **Get-IscsiConnection** into a PowerShell command window. You should see a listing similar to this showing that the server now has access to both iSCSIServerA and iSCSIServerB.

**Figure 92** PowerShell Get-iSCSIConnection

```

PS C:\Users\administrator.M50VSPEX> Get-IscsiConnection

ConnectionIdentifier : fffffa80657e7430-0
InitiatorAddress     : 10.10.21.21
InitiatorPortNumber  : 58817
TargetAddress        : 10.10.21.10
TargetPortNumber     : 3260
PSComputerName       :

ConnectionIdentifier : fffffa80657e7430-1
InitiatorAddress     : 10.10.20.21
InitiatorPortNumber  : 3264
TargetAddress        : 10.10.20.10
TargetPortNumber     : 3260
PSComputerName       :

ConnectionIdentifier : fffffa80657e7430-2
InitiatorAddress     : 10.10.21.21
InitiatorPortNumber  : 58561
TargetAddress        : 10.10.21.11
TargetPortNumber     : 3260
PSComputerName       :

ConnectionIdentifier : fffffa80657e7430-3
InitiatorAddress     : 10.10.20.21
InitiatorPortNumber  : 3008
TargetAddress        : 10.10.20.11
TargetPortNumber     : 3260
PSComputerName       :

PS C:\Users\administrator.M50VSPEX>

```

14. Ensure the devices have 2 paths for all the iSCSI shared storage. From an elevated PowerShell command window run:

**mpclaim -s -d**

Then choose an MPIO disk number and run:

**mpclaim -s -d 0**

Figure 93 PowerShell mpclaim.exe Configuration Output

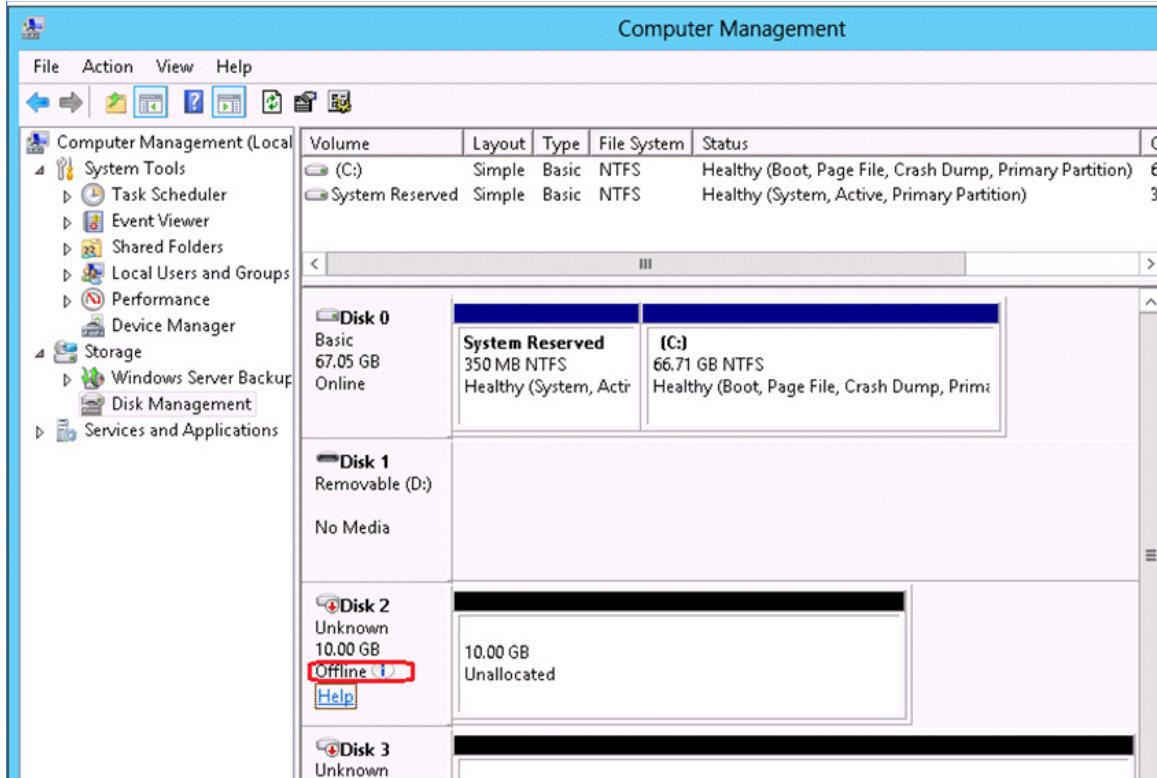
```

PS C:\Users\administrator.M50VSP&gt; mpclaim -s -d
For more information about a particular disk, use 'mpclaim -s -d #' where # is the MPIO disk number.
-----
MPIO Disk   System Disk  LB Policy  DSM Name
-----
MPIO Disk6   Disk 7       RR         Microsoft DSM
MPIO Disk5   Disk 6       RR         Microsoft DSM
MPIO Disk4   Disk 5       RR         Microsoft DSM
MPIO Disk3   Disk 4       RR         Microsoft DSM
MPIO Disk2   Disk 3       RR         Microsoft DSM
MPIO Disk1   Disk 2       RR         Microsoft DSM
MPIO Disk0   Disk 1       RR         Microsoft DSM
PS C:\Users\administrator.M50VSP&gt; mpclaim -s -d 0
MPIO Disk0: 02 Paths, Round Robin, ALUA Not Supported
Controlling DSM: Microsoft DSM
SN: 60648C458D6481C669B228CD6EA3D
Supported Load Balance Policies: F00 RR RRWS LQD WP LB
-----
Path ID      State           SCSI Address    Weight
-----
0000000077050001 Active/Optimized 005|000|001|007 0
0000000077050000 Active/Optimized 005|000|000|007 0
PS C:\Users\administrator.M50VSP&gt; mpclaim -s -d 1
MPIO Disk1: 02 Paths, Round Robin, ALUA Not Supported
Controlling DSM: Microsoft DSM
SN: 60648C1D454935ADDEA7DADF795A3
Supported Load Balance Policies: F00 RR RRWS LQD WP LB
-----
Path ID      State           SCSI Address    Weight
-----
0000000077050001 Active/Optimized 005|000|001|008 0
0000000077050000 Active/Optimized 005|000|000|008 0
PS C:\Users\administrator.M50VSP&gt; mpclaim -s -d 2
MPIO Disk2: 02 Paths, Round Robin, ALUA Not Supported
Controlling DSM: Microsoft DSM
SN: 60648CF5B07CEB1EC9A3802B5D6059
Supported Load Balance Policies: F00 RR RRWS LQD WP LB
-----
Path ID      State           SCSI Address    Weight
-----
0000000077050001 Active/Optimized 005|000|001|009 0
0000000077050000 Active/Optimized 005|000|000|009 0
PS C:\Users\administrator.M50VSP&gt;

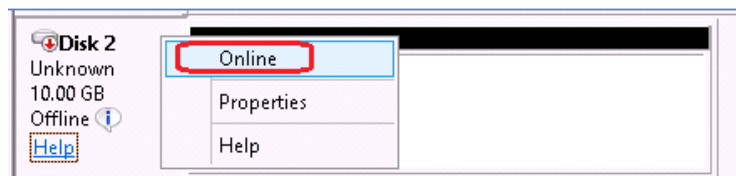
```

15. Login to the Windows Hyper-V host and open Server Manager. In Server Manager, expand Storage and choose **Disk Management**. In the Disk Management right window pane, you will see all the iSCSI LUNs listed as Unknown and Offline.

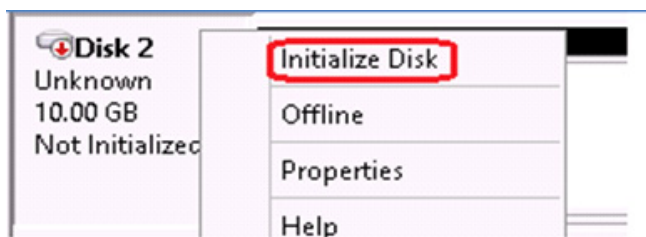


**Figure 94** *Disk Management - Disk Offline*

16. Right-click in the left-hand of the display for the first iSCSI LUN disk and choose **Online**.

**Figure 95** *Disk Management - Disk Online*

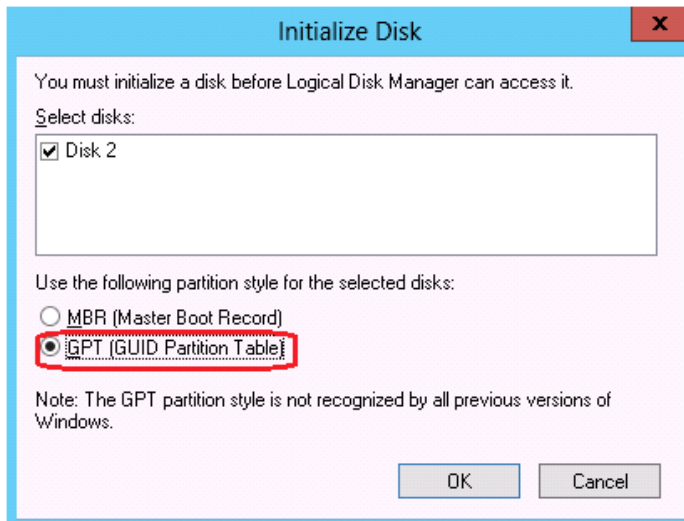
17. Repeat the step 16 for all the remaining iSCSI LUNs which are offline.
18. Right-click in the left-hand of the display for the same disk and select **Initialize Disk**. You can all initialize all iSCSI LUNs one time.

**Figure 96** *Disk Management - Initialize Disk*



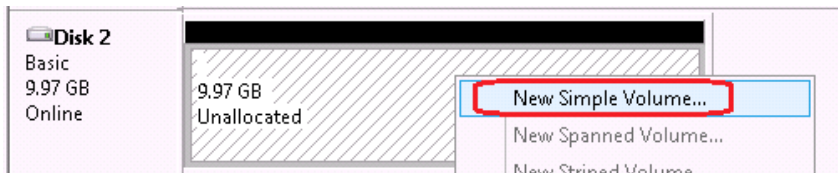
19. There are two options for creating a partition on the selected disk – MBR or GPT. If the volume is over 2 TB in size, MBR is not an option. GPT partitions have some additional fault tolerance that MBR partitions do not have. Either type of partition works, but you may want to choose GPT partitions for use in the cluster. Click **OK**. Repeat this step for all the remaining iSCSI LUNs.

**Figure 97** *Disk Management - Initialize Disk MBR/GPT*

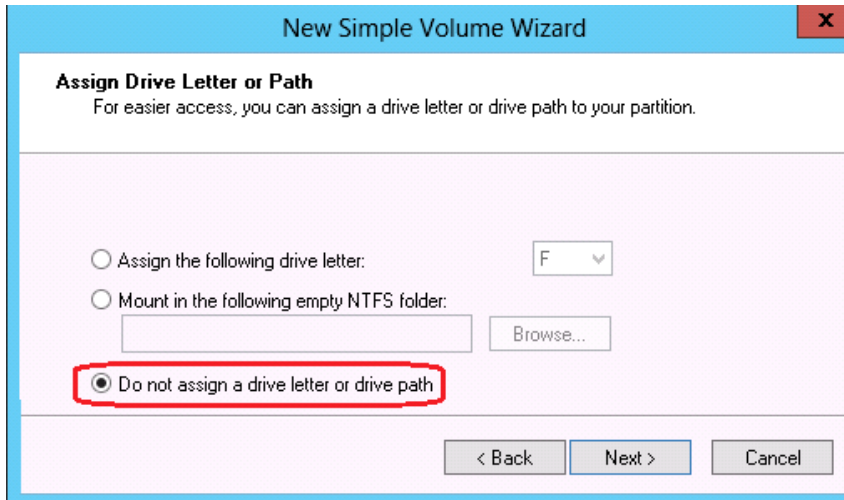


20. Once all the disks are initialized, format with the NTFS file system and assign drive letters to them.  
 21. Right-click in the right-hand of the display for the same disk. Select **New Simple Volume**.

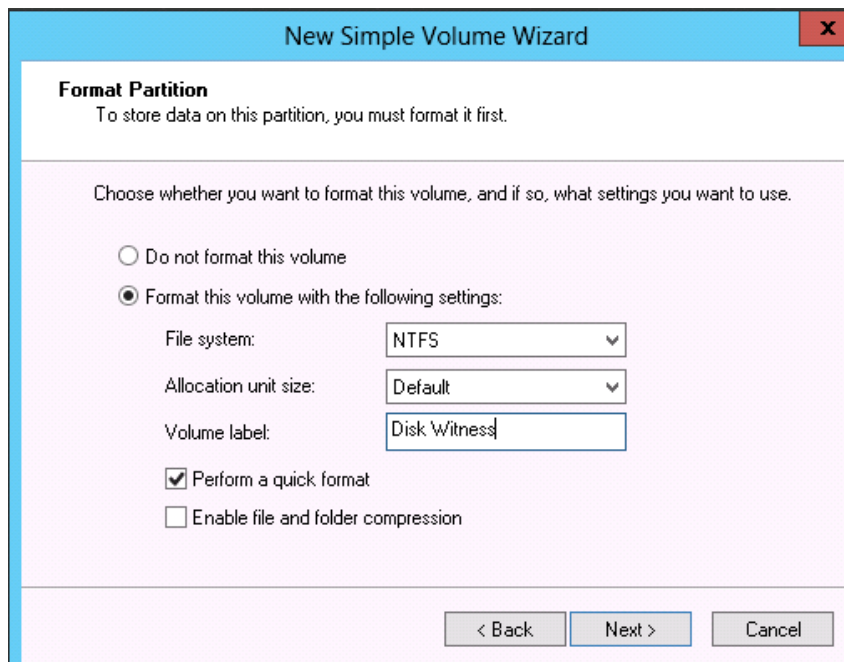
**Figure 98** *Disk Management - New Simple Volume*



22. Click **Next** on the welcome window of the New Simple Volume Wizard.  
 23. Click **Next** on the Specify Volume Size window to create the maximum sized volume.  
 24. Click **Do not assign a driver path** on the Assign Drive Letter or Path window.

**Figure 99** *Disk Management - New Simple Volume Wizard*

25. Click **Next**.
26. Accept the defaults on the Format Partition window by clicking on **Next**.
27. Click **Finish** on the Summary window.
28. Assign a Volume label. Accept the other defaults on the Format Partition window by clicking on **Next**.

**Figure 100** *Format Partition - New Simple Volume Wizard*

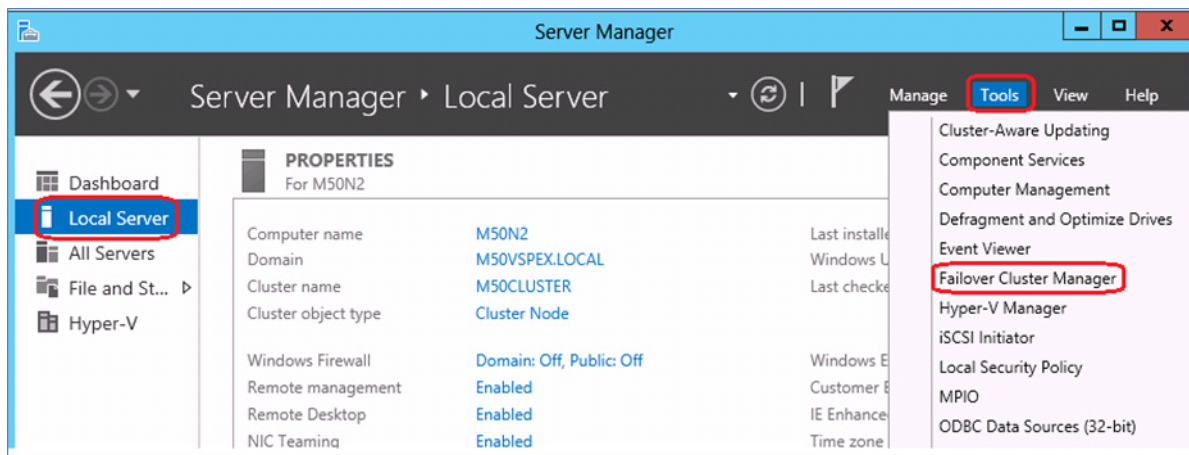
29. Click **Finish** on the Summary window.
30. Right-click the left-hand side of the display for the disk and select **Offline**.

31. Repeat the above steps for each of the iSCSI LUNs to be used by the cluster.
32. This initialization and formatting process only needs to be done from a single node of the cluster.
33. It is a good practice to logon to each node of the cluster and run diskmgmt.msc to validate each node has access to the shared storage.

### 12.3 Microsoft Failover Cluster Validation

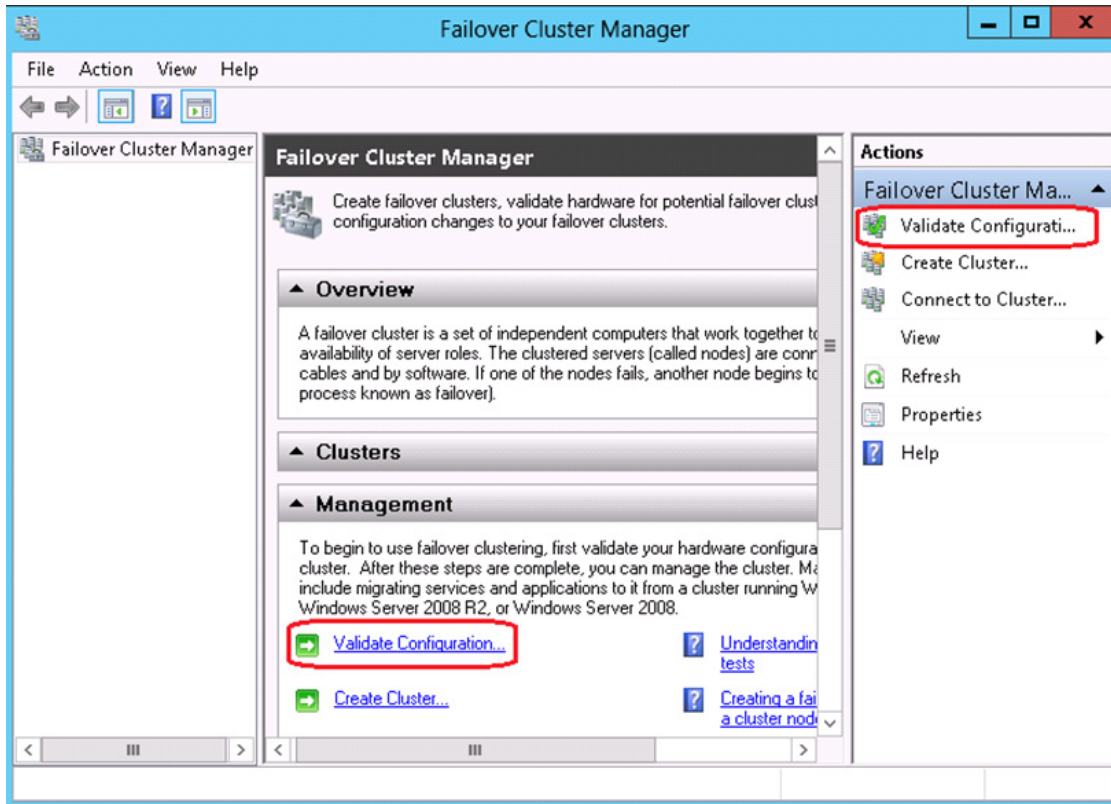
1. Login to a node using a domain administrative account with local privileges.
2. From **Server Manager**, select **Local Server**. From the **Tools** menu, select **Failover Cluster Manager**.

**Figure 101**      **Server Manager**



3. In the **Failover Cluster Manager** window. Select **Validate Configuration**, and then click **Next**.

Figure 102 Failover Cluster Manager



4. In the **Validate a Configuration Wizard**, click **Next**.
5. Add all the nodes one at a time into the **Enter Name** text field, and click **Next**.

**Figure 103**      **Validate a Configuration Wizard**

6. In the **Validate a Configuration Wizard**, select **Run All Tests** and click **Next**.
7. Confirm the settings and click **Next** to start the validation of tests.



**Note** The validation stage of the cluster creation may take up to an hour to complete, depending on the number of nodes and disks.

8. Review the report and resolve any issues found by the validation wizard before continuing.
9. Click **Finish**.

Figure 104 Failover Cluster Validation Report



## Failover Cluster setup

1. 1. In the Failover Cluster Manager, click **Create a Cluster**.
2. 2. In the Welcome screen, click **Next**.
3. 3. In the **Create Cluster Wizard > Select Servers** window, add all the nodes one at a time into the **Enter server name** text field and click **Next**

**Figure 105** *Create Cluster Wizard*

4. In the **Create Cluster Wizard > Validation Warning** window, Select **No** to skip the Validation tests.
5. In the **Create Cluster Wizard > Access Point for Administering the Cluster** window, Enter the Cluster Name, Cluster IP, and click **Next**.

**Figure 106** *Specify Network Name and IP Address in Create Cluster Wizard*

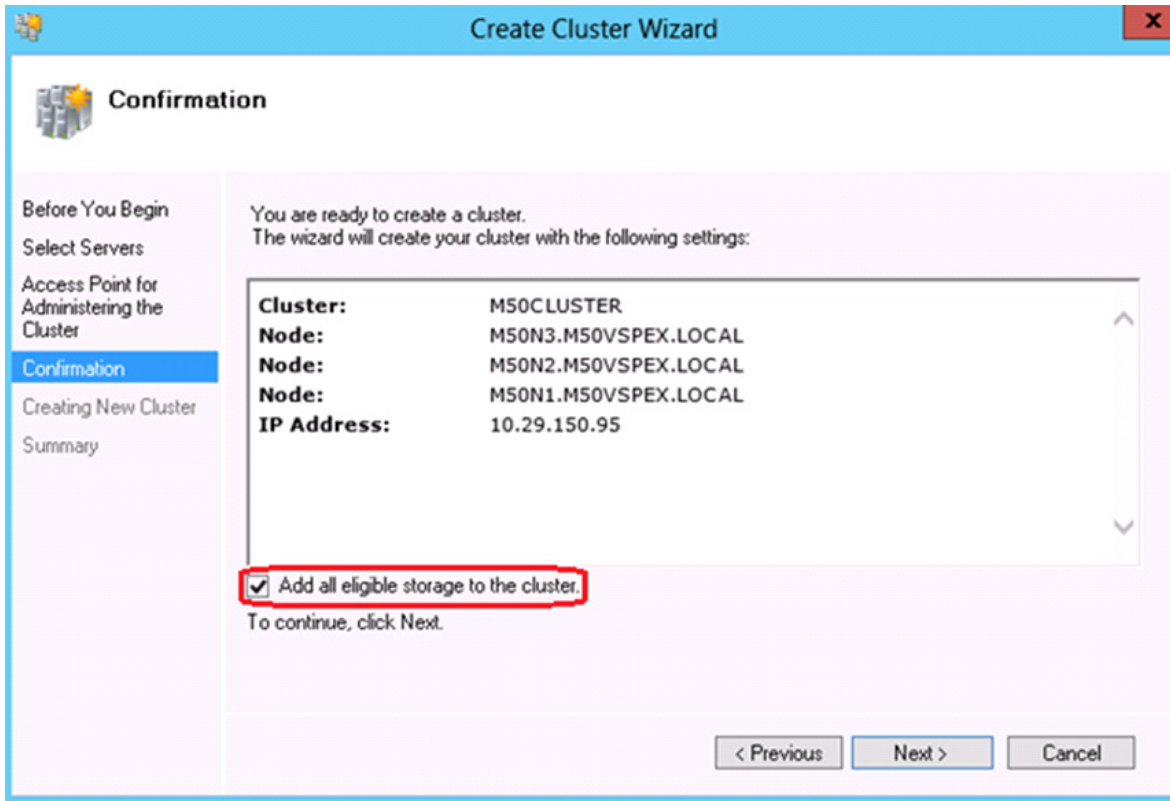
	Networks	Address
<input checked="" type="checkbox"/>	10.29.150.0/24	10.29.150.95

At the bottom are '< Previous', 'Next >', and 'Cancel' buttons.



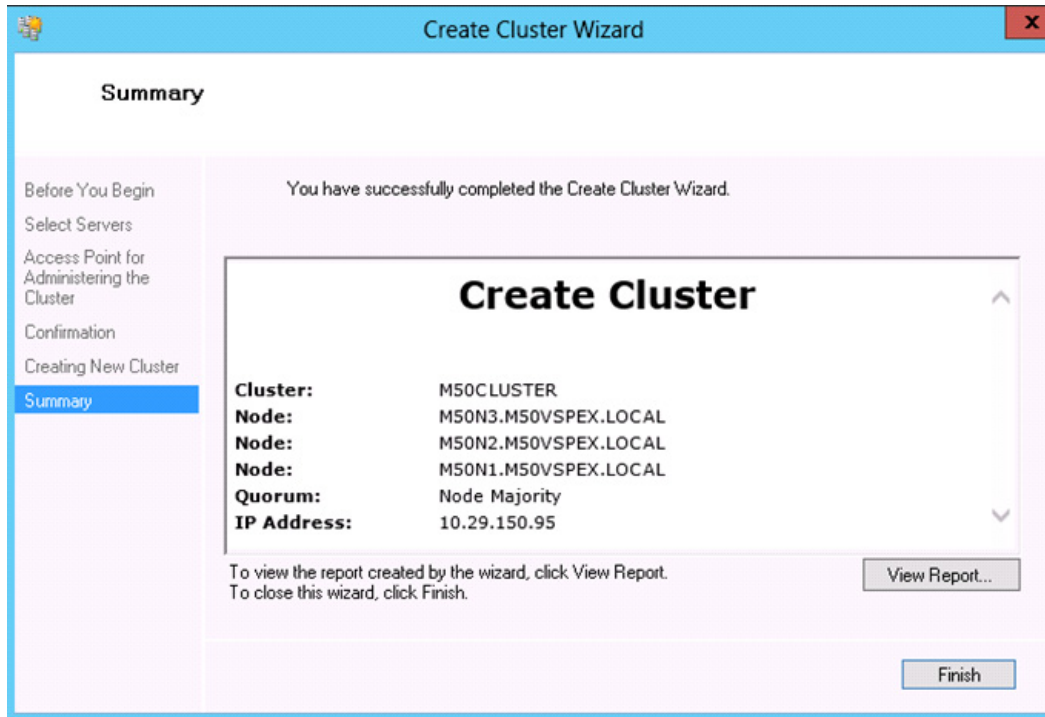
6. In the **Create Cluster Wizard > Confirmation** window, review the settings and select **Add all eligible storage to the cluster**. Click **Next**.

**Figure 107** Confirmation Page in Create Cluster Wizard



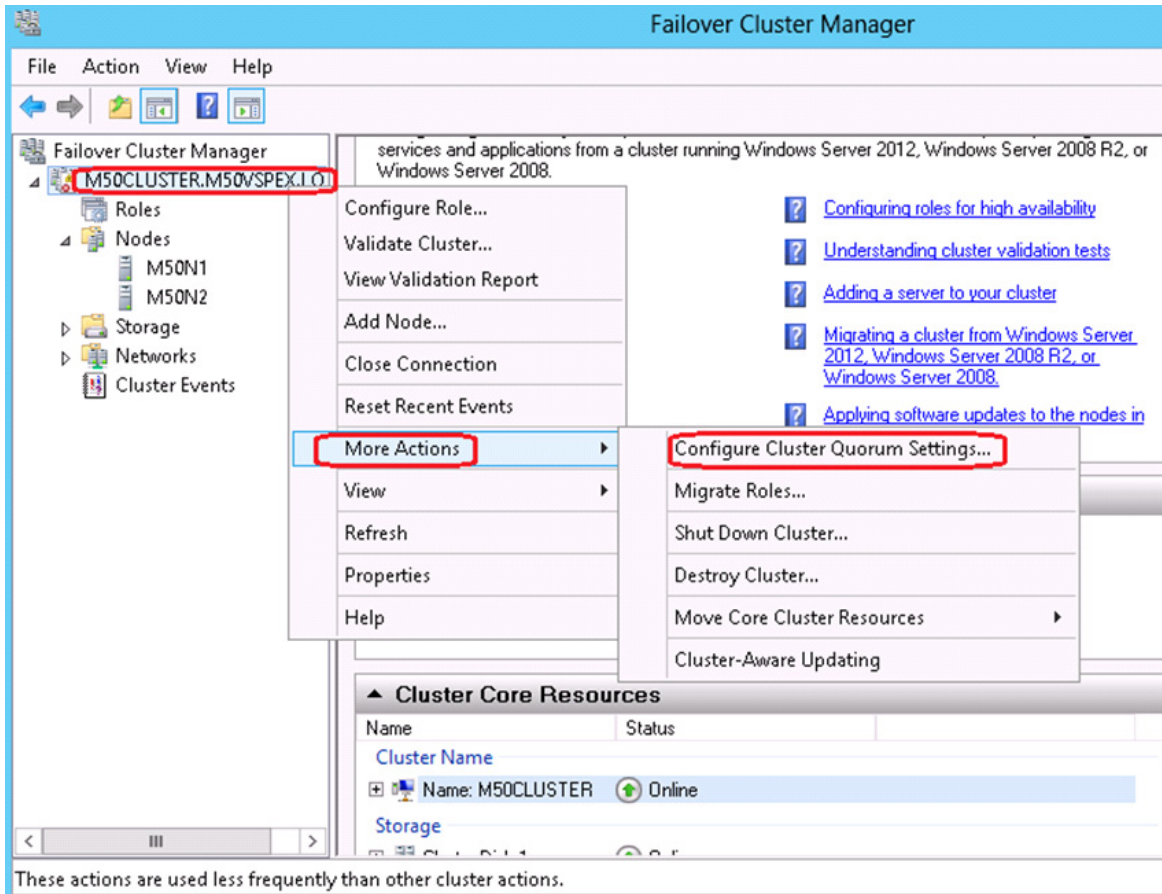
7. In the Summary page, click **finish**.

**Figure 108** Summary Page in Create Cluster Wizard

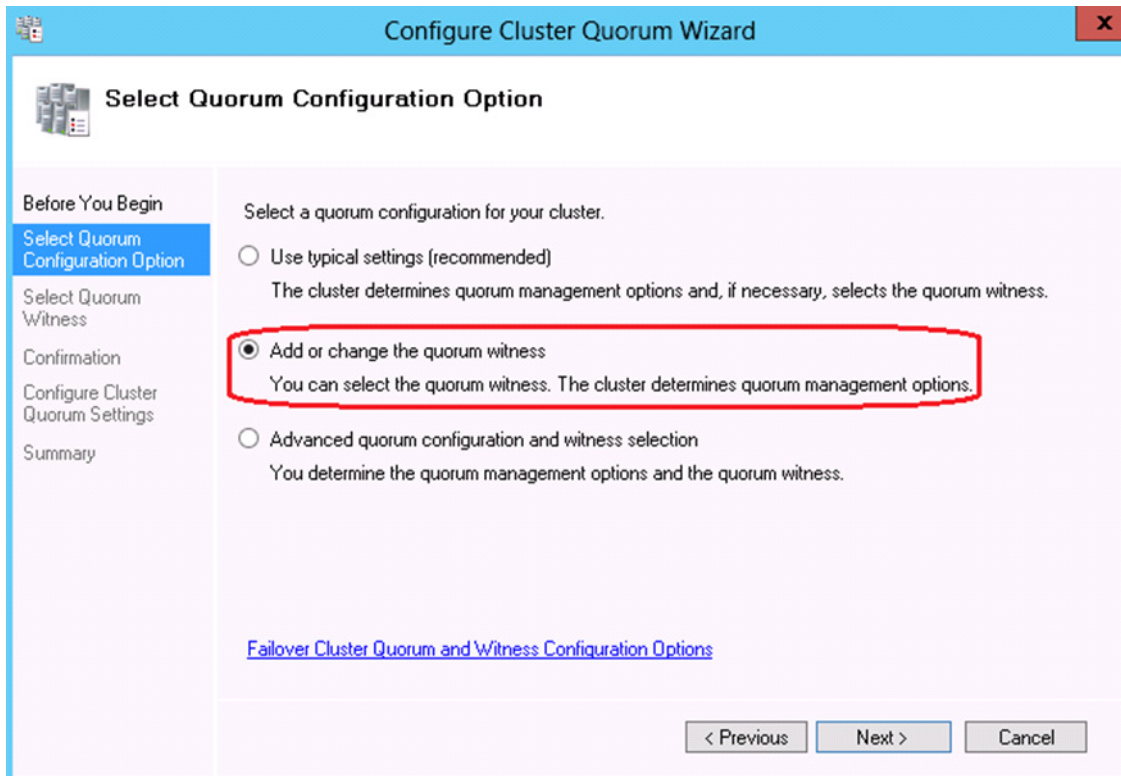


8. In the Failover Cluster Manager, right-click the cluster name, Choose More Actions, Configure Cluster Quorum Settings and click **Next**.

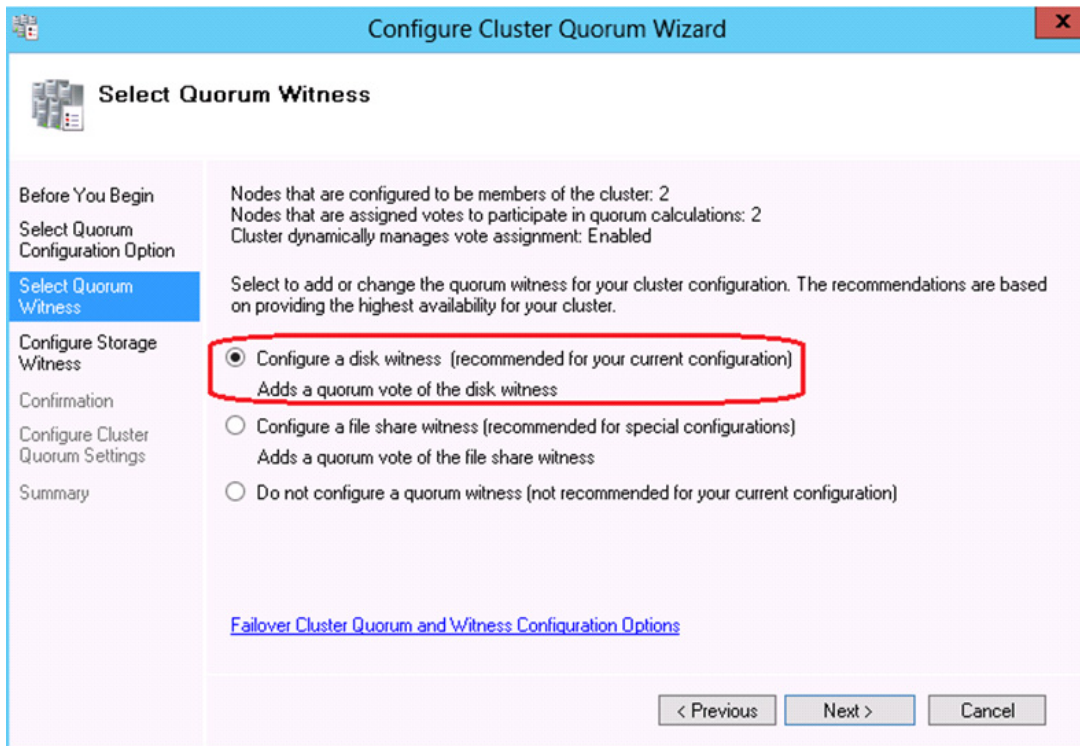
**Figure 109** *Failover Cluster Manager*



9. In the **Configure Cluster Quorum Wizard > Before You Begin** window, click **Next**.
10. In the **Configure Cluster Quorum Wizard > Select Quorum Configuration Option** window, click **Add or change the quorum witness** and click **Next**.

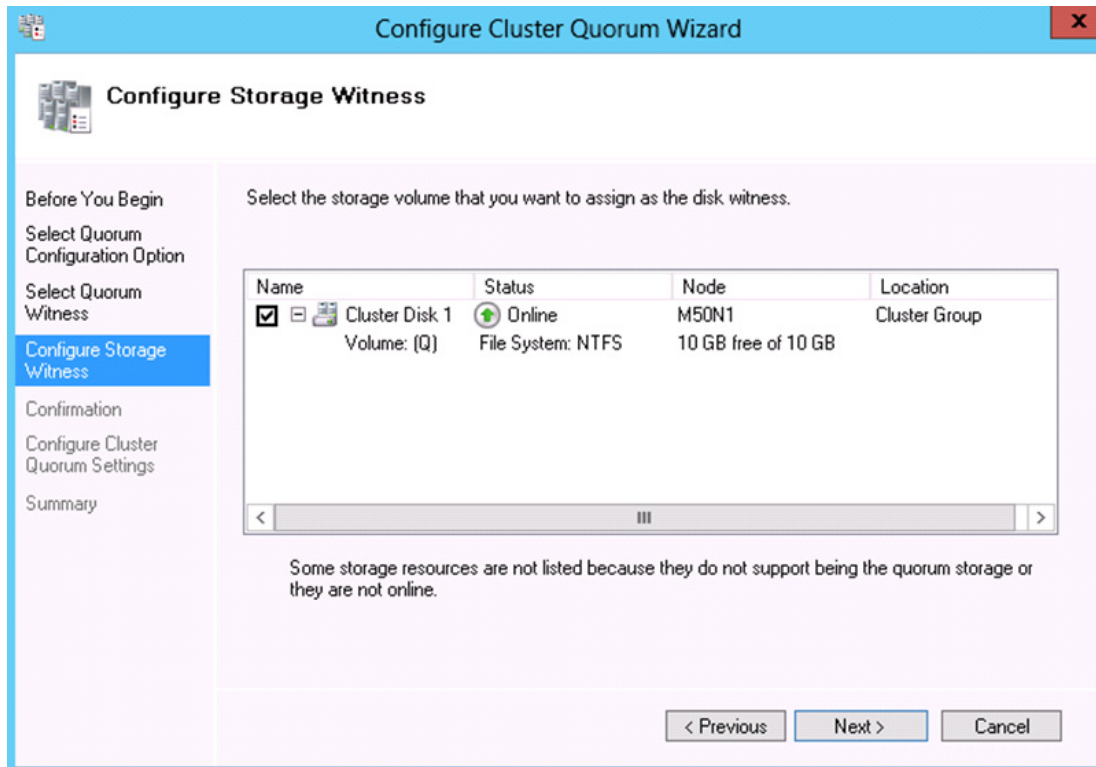
**Figure 110**      **Select Quorum Configuration Option**

11. In the **Configure Cluster Quorum Wizard > Select Quorum Witness** window, **Select Configure a disk witness.**

**Figure 111** *Configure Cluster Quorum Wizard*

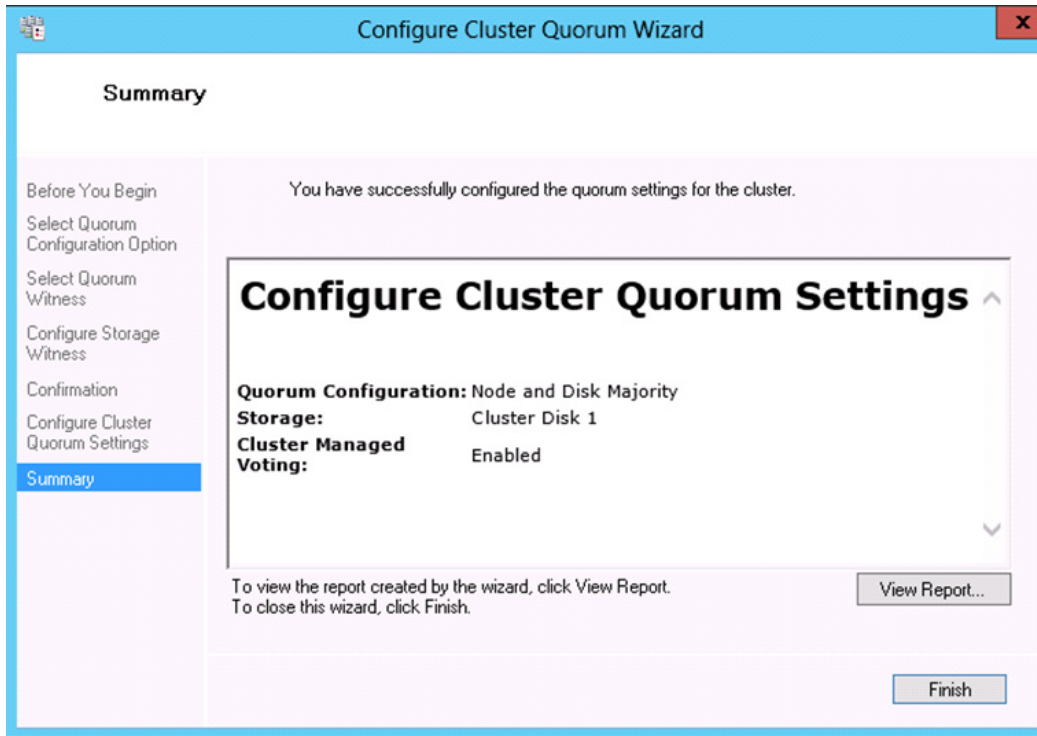
12. In the **Configure Cluster Quorum Wizard > Configure Storage Witness** page, select the 10GB disk and click **Next**.

**Figure 112**      **Configure Storage Witness in Configure Cluster Quorum Wizard**



13. In the **Confirmation** Page click **Next**.
14. And, in the **Summary** page click **Finish**.

Figure 113 Configure Cluster Quorum Wizard - Summary



The recommended quorum modes for even and odd nodes are:

- For even number of nodes (2, 4, 6,...), select Node and Disk Majority.
- For odd number of nodes (3, 5, 7,...), select Node Majority.<sup>1</sup>

For more information on Best Practices for configuring quorum in a failover cluster:

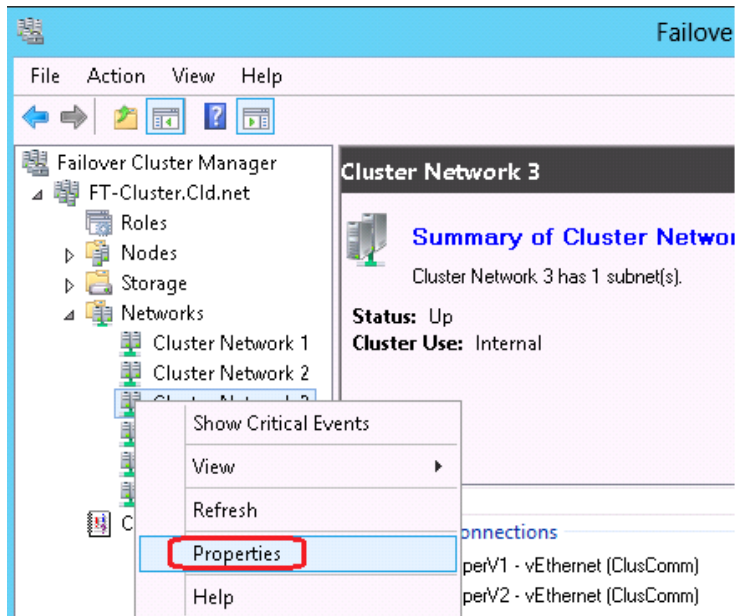
[http://technet.microsoft.com/en-us/library/cc770620\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc770620(v=ws.10).aspx)

15. Within **Server Manager** on the configuration workstation, click **Tools** and select **Failover Cluster Manager**. Select **Connect to Cluster...**
16. In the **Select Cluster** window that opens, enter the name of the cluster you just created. Click **OK** to continue.
17. Verify that all Cluster Networks are assigned, the shared storage disks appear properly and the status shows online.
18. Though not a requirement, rename the networks as per their intended use for easy identification and troubleshooting purposes. Right-click the network and select **Properties**.

1.

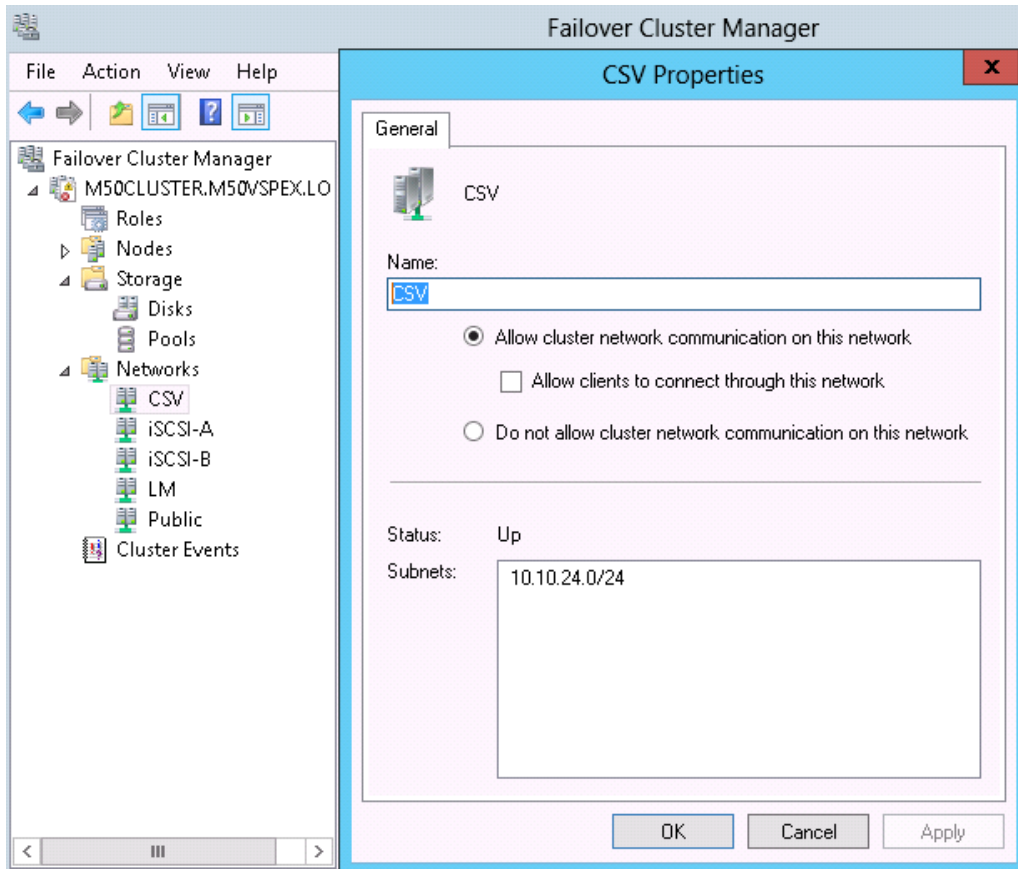


**Figure 114**      *Rename Networks in Failover Cluster Manager*



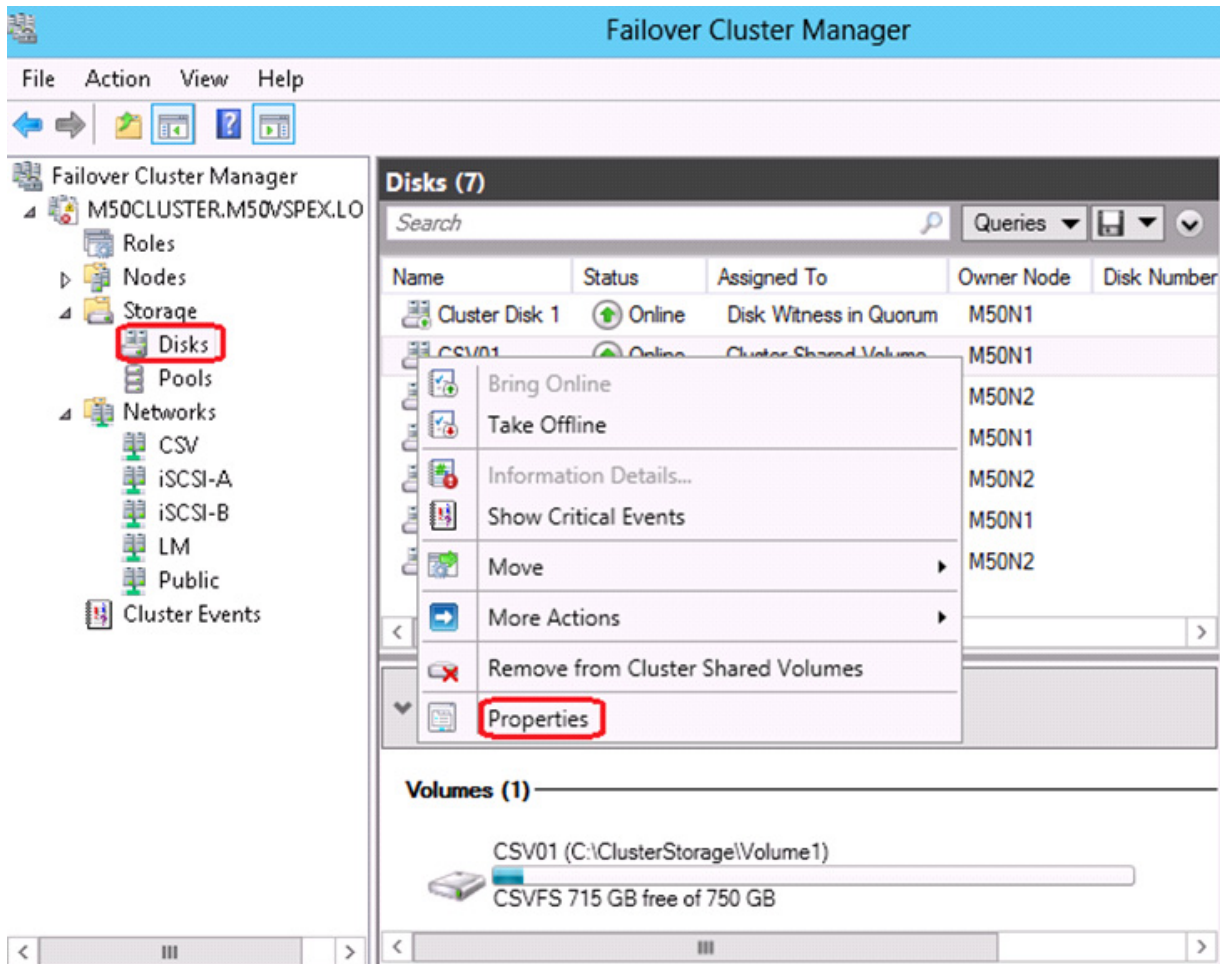
19. Enter the name of the network as defined on the nodes. Click **OK**. Repeat for all networks.

**Figure 115**      **Network Properties in Failover Cluster Manager**



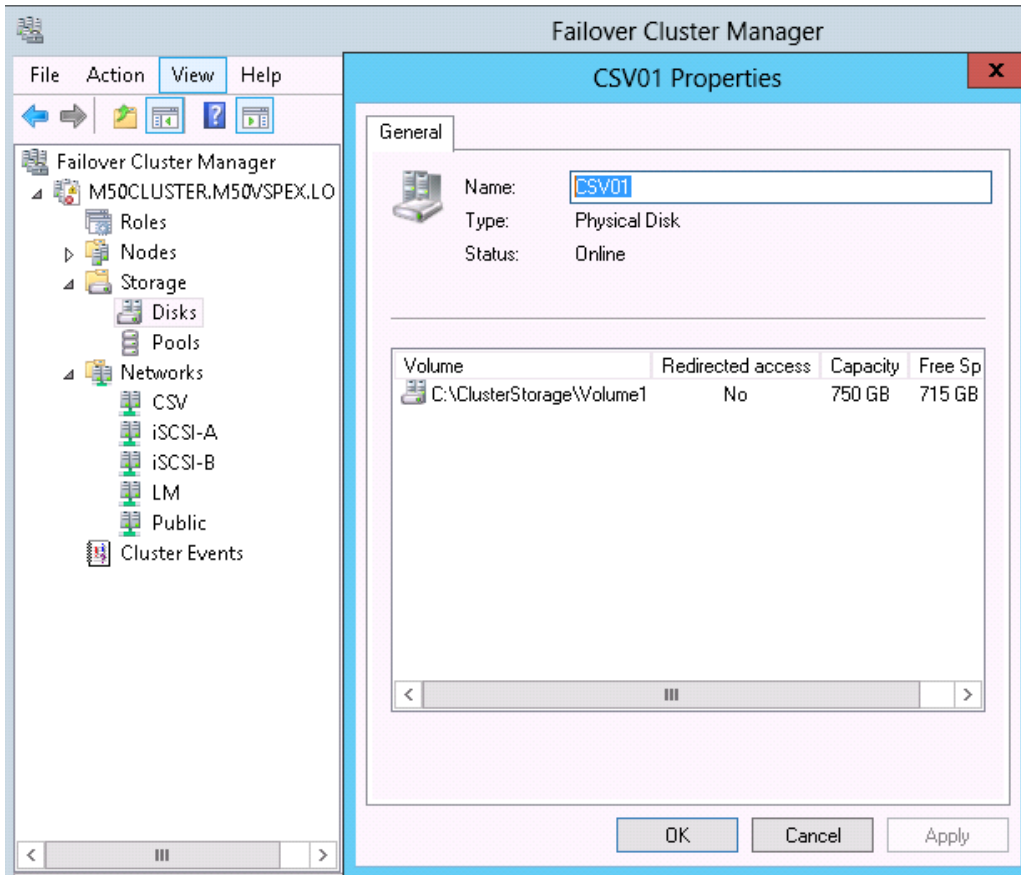
20. Though not a requirement, rename the Disks also by Right-click the Disks and select **Properties**.

Figure 116 Failover Cluster Manager - Disks



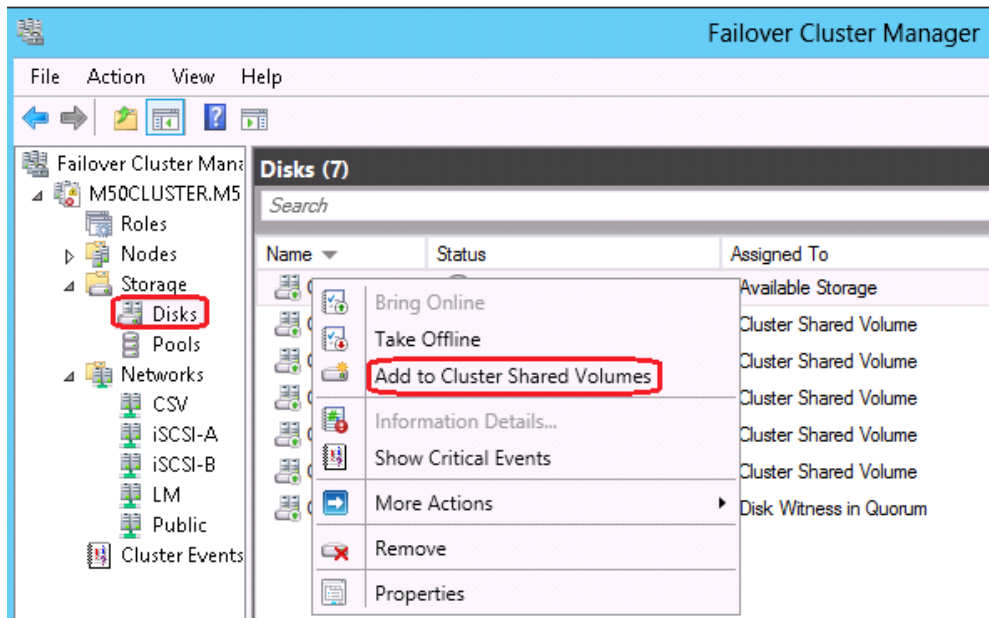
21. Rename the Disk and click **Next**. It is a good practice to rename the disk as the volume name.

**Figure 117**      **Failover Cluster Manager - Disks Properties**



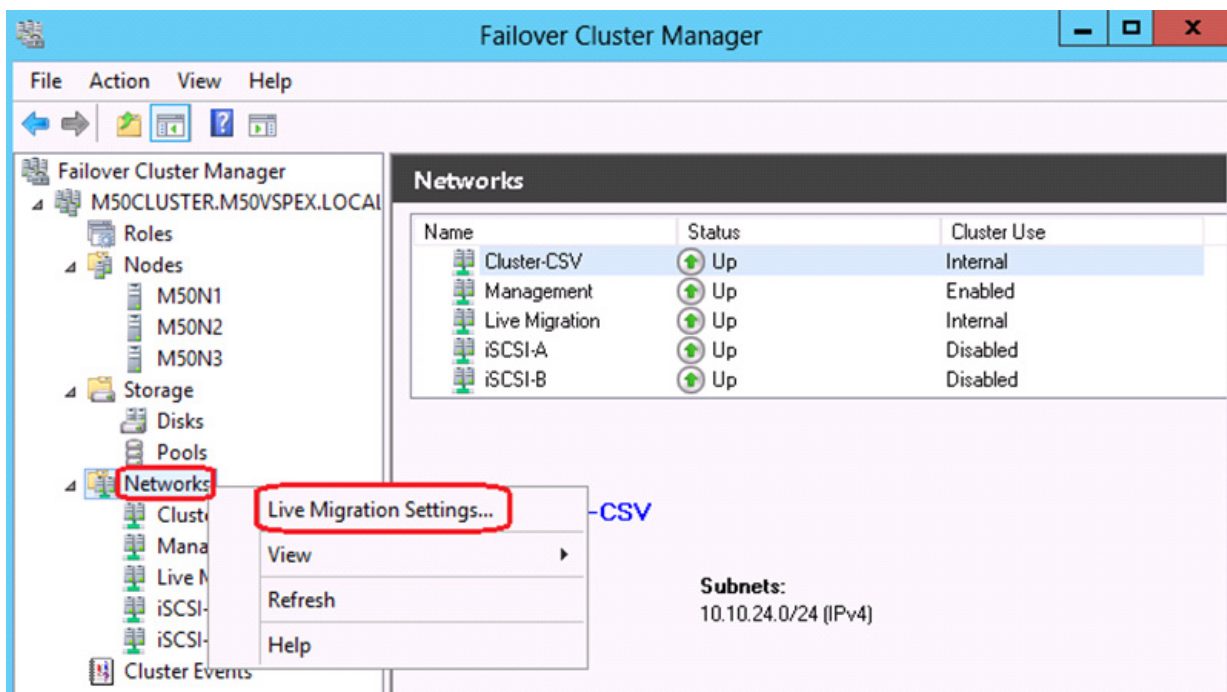
22. To add Cluster Shared Volume, open Failover Cluster Manager from any cluster node.
23. Select the disk that will be used for storing the virtual machines. Right-click and **select Add to Cluster Shared Volumes**.

Figure 118 Failover Cluster Manager - Add to CSV



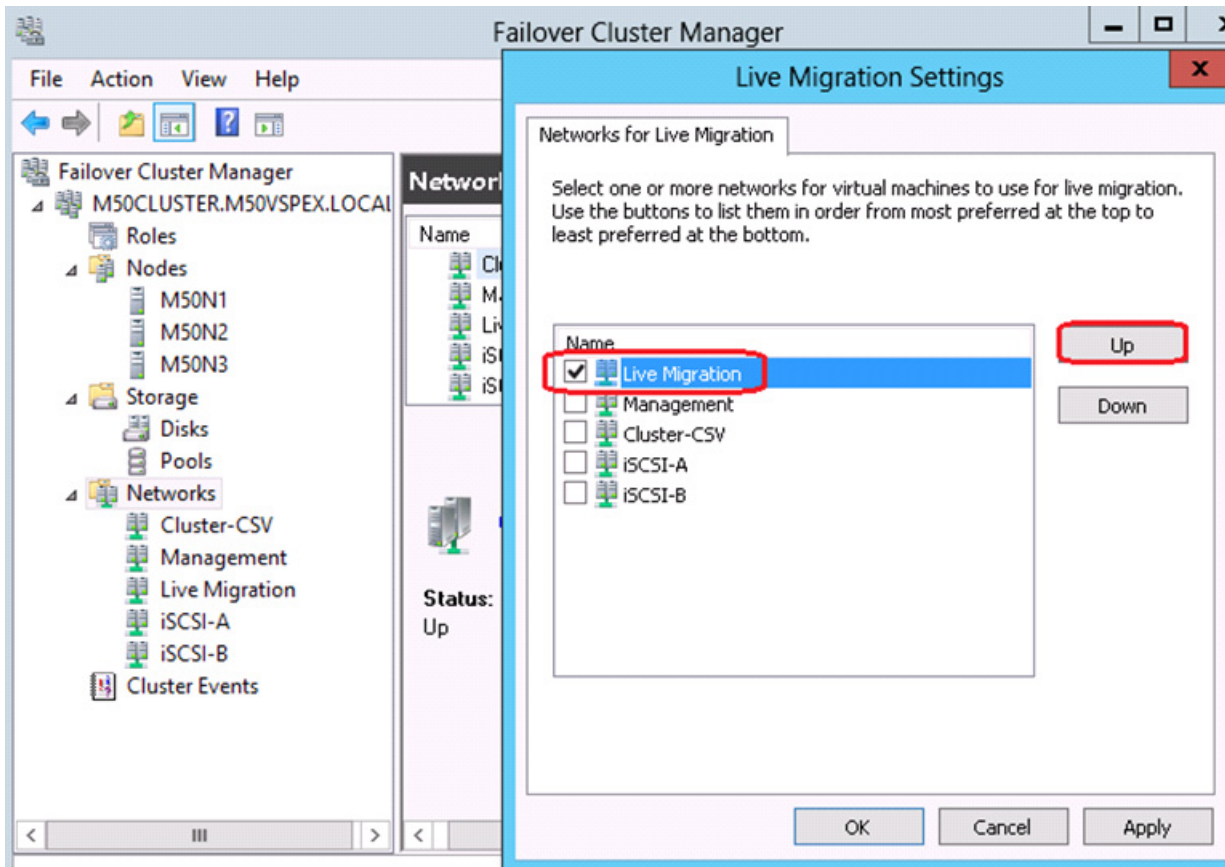
24. Repeat the above step 23 for all disks that will storing virtual machines.
25. To configure the network for Live Migration, right click **Networks** and select **Live Migration Settings...**

Figure 119 Failover Cluster Manager - Networks



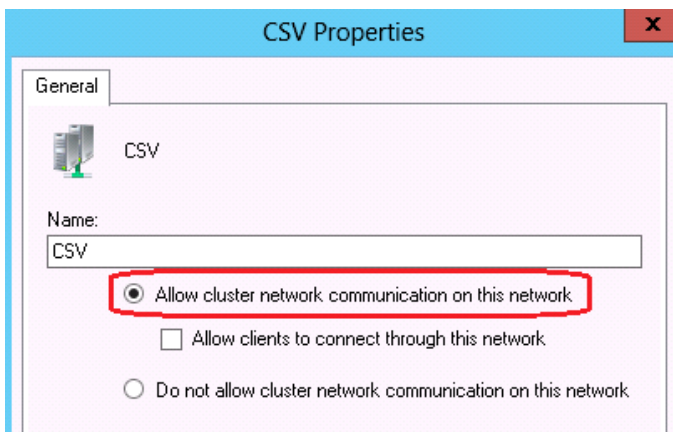
26. Select the network for **Networks for Live Migration** and move **UP** to the top in the order. Deselect other networks.

**Figure 120** *Failover Cluster Manager - Live Migration Settings*

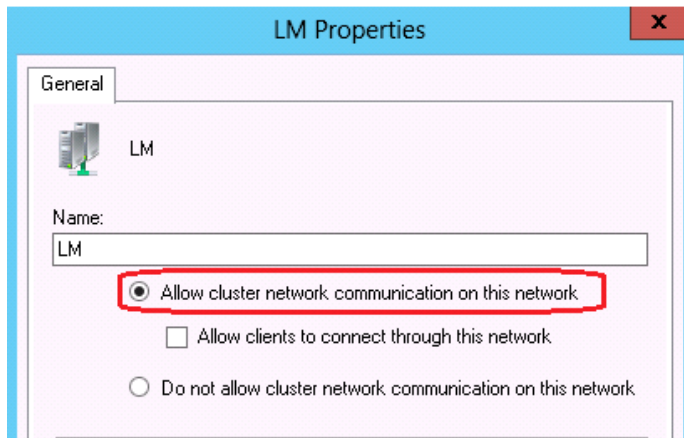


27. For Cluster and CSV network, use the highlighted option as shown in [Figure 121](#).

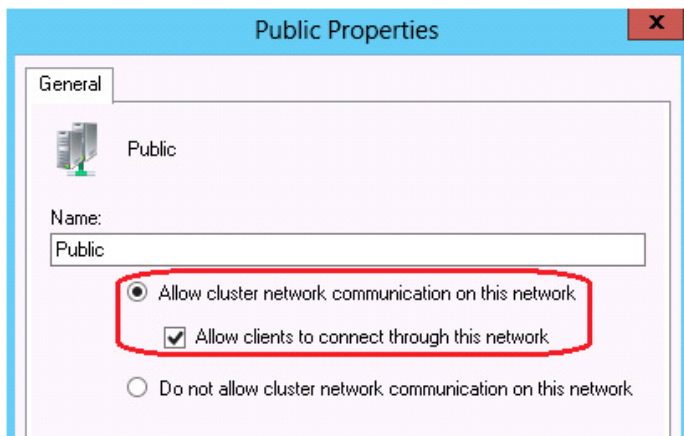
**Figure 121** *Failover Cluster Manager - CSV Networks Properties*



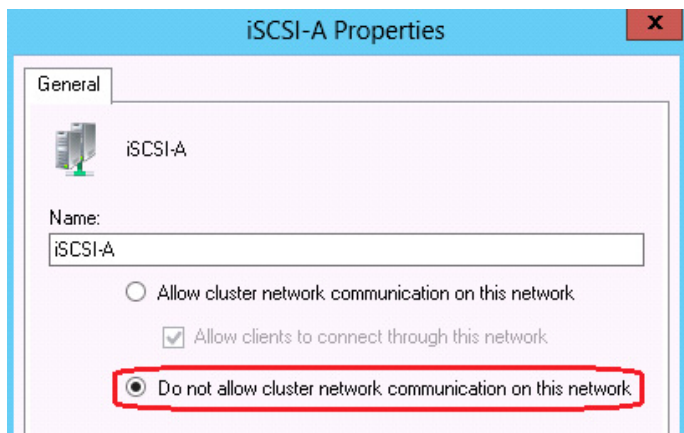
28. For Live Migration network, use the highlighted option as shown in [Figure 122](#).

**Figure 122** *Failover Cluster Manager - LM Networks Properties*

29. For Public/Management network, use the highlighted option as shown in [Figure 123](#).

**Figure 123** *Failover Cluster Manager - Public Networks Properties*

30. For iSCSI network, the highlighted option as shown in [Figure 124](#).

**Figure 124** *Failover Cluster Manager - iSCSI Networks Properties*



## Create Virtual Machine

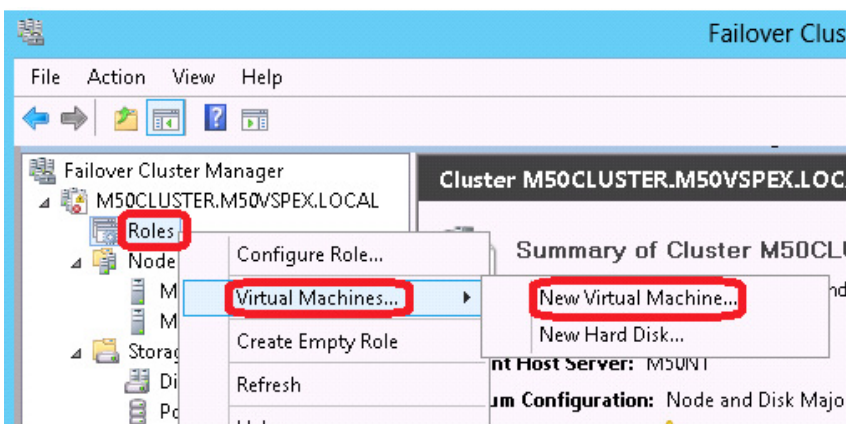
This section describes how to create the first virtual machine. This first virtual machine will be turned into a template that can be used to quickly create additional virtual machines. To build the template, follow these steps:

1. Create a generic virtual machine.
2. Install Windows Server 2012.
3. Customize the virtual machine to meet your base standards, including things like firewall settings, management utilities, network definitions, and so forth.
4. Run Microsoft's sysprep utility on the machine to prepare it for cloning.
5. Store the virtual machine in a library location for later cloning.

Follow these steps from one of the nodes of the cluster:

1. From **Failover Cluster Manager**, right-click **Roles**, select **Virtual Machines**, then **New Virtual Machine...**

**Figure 125** *Failover Cluster Manager - Roles*



2. In the **New Virtual Machine** window, select one of the nodes in the cluster.
3. Click **Next** on the Before You Begin window of the New Virtual Machine Wizard.
4. On the **Specify Name and Location** windows, enter a name for your VM Template.
5. Check the check box next to **Store the virtual machine in a different location**.

**Figure 126**      **New Virtual Machine Wizard**

The screenshot shows the 'New Virtual Machine Wizard' window with the 'Specify Name and Location' step selected in the left-hand navigation pane. The main area contains instructions and input fields. The 'Name' field is set to 'TemplateVM'. The 'Location' field is set to 'C:\ClusterStorage\Volume2\'. A red box highlights the checkbox 'Store the virtual machine in a different location' and the 'Browse...' button. A warning icon and text are present below the location field.

**Specify Name and Location**

Before You Begin  
Specify Name and Location  
Assign Memory  
Configure Networking  
Connect Virtual Hard Disk  
Installation Options  
Summary

Choose a name and location for this virtual machine.


The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name:

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☒ Store the virtual machine in a different location

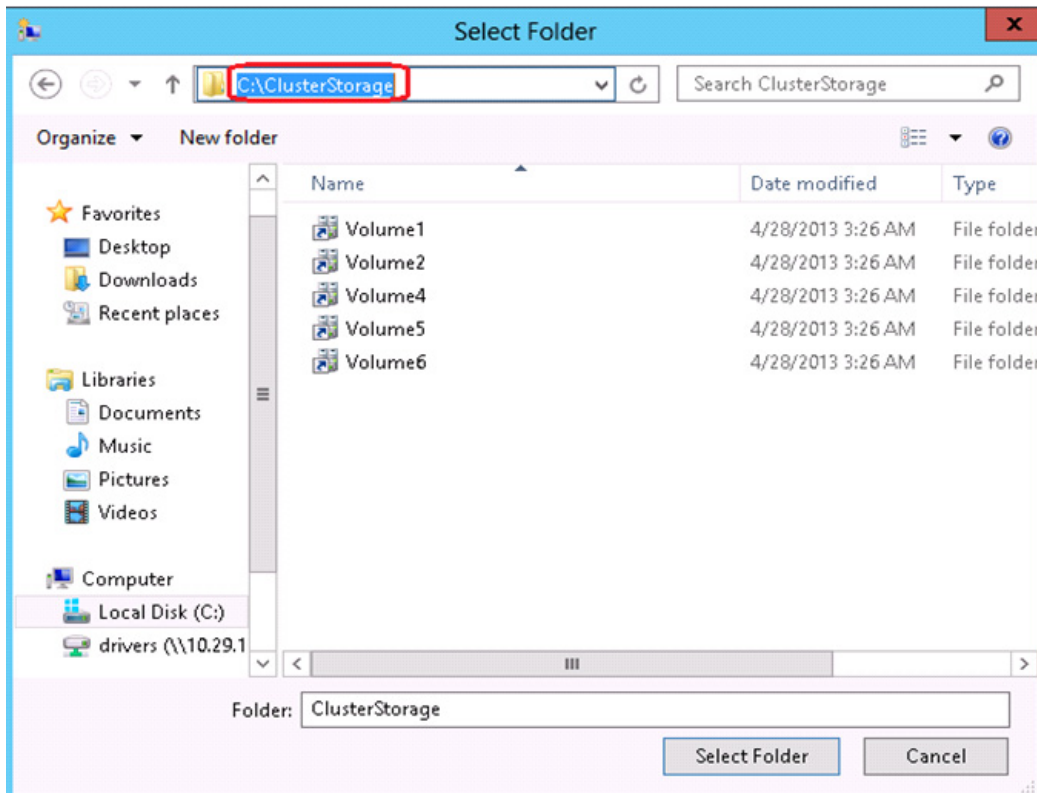
Location:

 If you plan to take snapshots of this virtual machine, select a location that has enough free space. Snapshots include virtual machine data and may require a large amount of space.

< Previous   Next >   Finish   Cancel

6. Click **Browse** to select the location to store the virtual machine files.

Figure 127 Windows Explorer - Browse



7. From the Windows Explorer window, navigate to C:\ClusterStorage. There is one subdirectory under ClusterStorage for each CSV. Select any one of them.
8. Click **Select Folder** to continue.
9. Back in the New Virtual Machine Wizard, click **Next**.
10. On the **Assign Memory** window, you can leave the value of Startup memory at the default of 512, or you can expand it to give it more memory at startup.
11. Check the box to Use Dynamic Memory for this virtual machine. Click **Next** to continue.

**Figure 128**      *Assign Memory in New Virtual Machine Wizard*

The screenshot shows the 'Assign Memory' step of the 'New Virtual Machine Wizard'. The left sidebar contains a list of steps: 'Before You Begin', 'Specify Name and Location', 'Assign Memory' (highlighted), 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains instructions: 'Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 8 MB through 123308 MB. To improve performance, specify more than the minimum amount recommended for the operating system.' Below this, the 'Startup memory' is set to '1024 MB'. A checkbox labeled 'Use Dynamic Memory for this virtual machine' is checked. A red box highlights the 'Startup memory' field and the checked checkbox. A red box also highlights the 'Use Dynamic Memory for this virtual machine' checkbox.

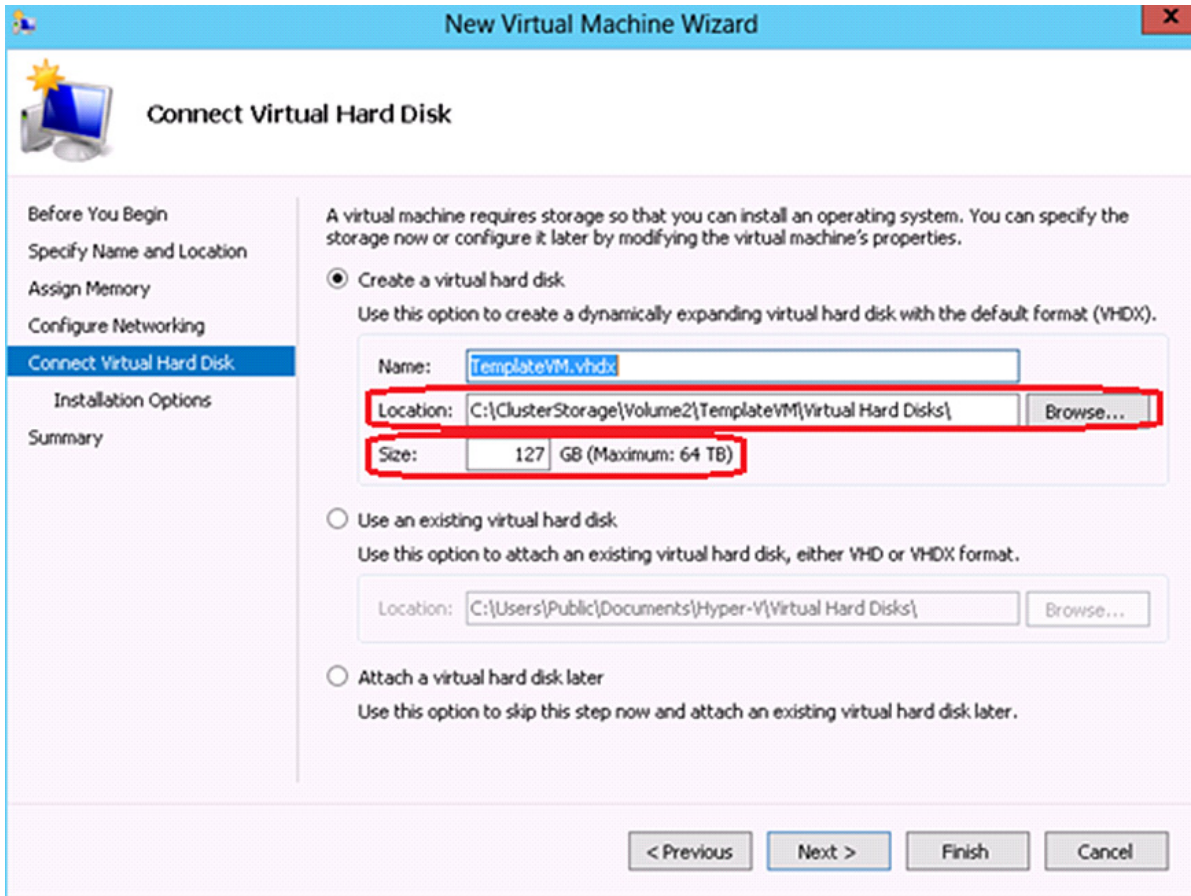
12. In the **Configure Networking** window, select the Connection from the drop-down list that matches the name of the virtual NIC used for accessing the VMs. Click **Next** to continue.

**Figure 129**      *Configure Networking in New Virtual Machine Wizard*

The screenshot shows the 'Configure Networking' step of the 'New Virtual Machine Wizard'. The left sidebar contains a list of steps: 'Before You Begin', 'Specify Name and Location', 'Assign Memory', 'Configure Networking' (highlighted), 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains instructions: 'Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.' Below this, the 'Connection' dropdown menu is open, showing 'VMComm' as the selected option. A red box highlights the 'VMComm' option in the dropdown list.

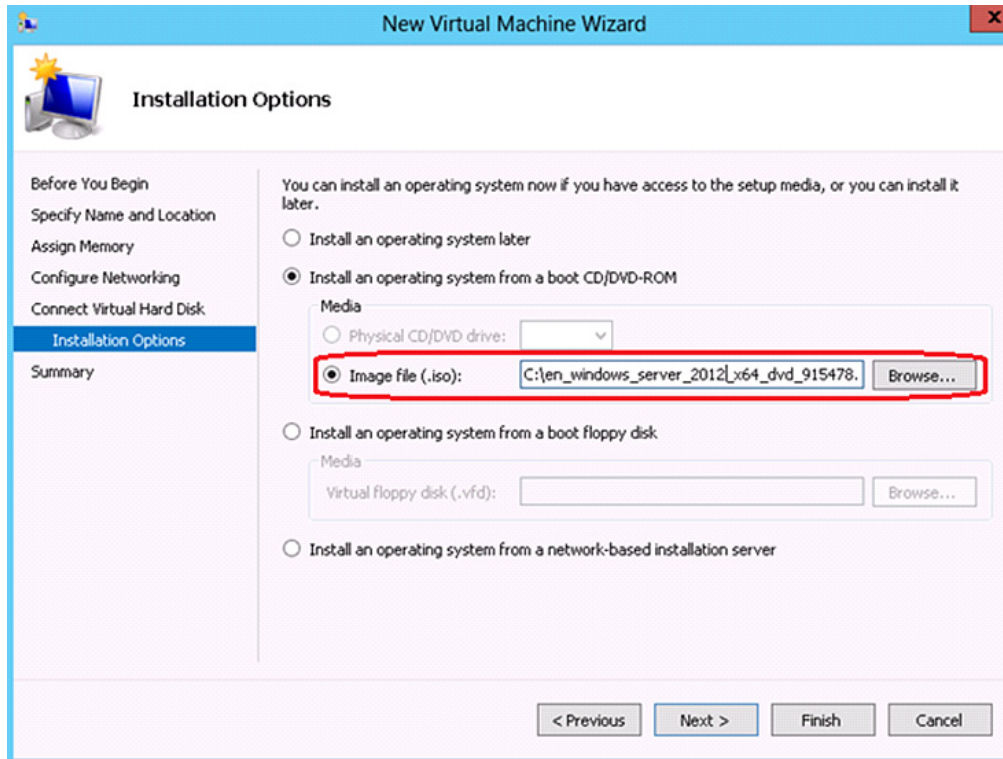
13. In the **Connect Virtual Hard Disk** window, you can leave the default size of the virtual hard drive as 127 GB or enter a new value as per your requirement. Click **Next** to continue.

Figure 130 Connect VHD in New Virtual Machine Wizard



14. In the **Installation Options** window, select the radio button by **Install an operating system from a boot CD/DVD-ROM**. Ensure the radio button next to **Image File (.iso)** is selected.
15. Click **Browse** and select the .iso file for the Windows Server 2012 installation media and click **Next** to continue.

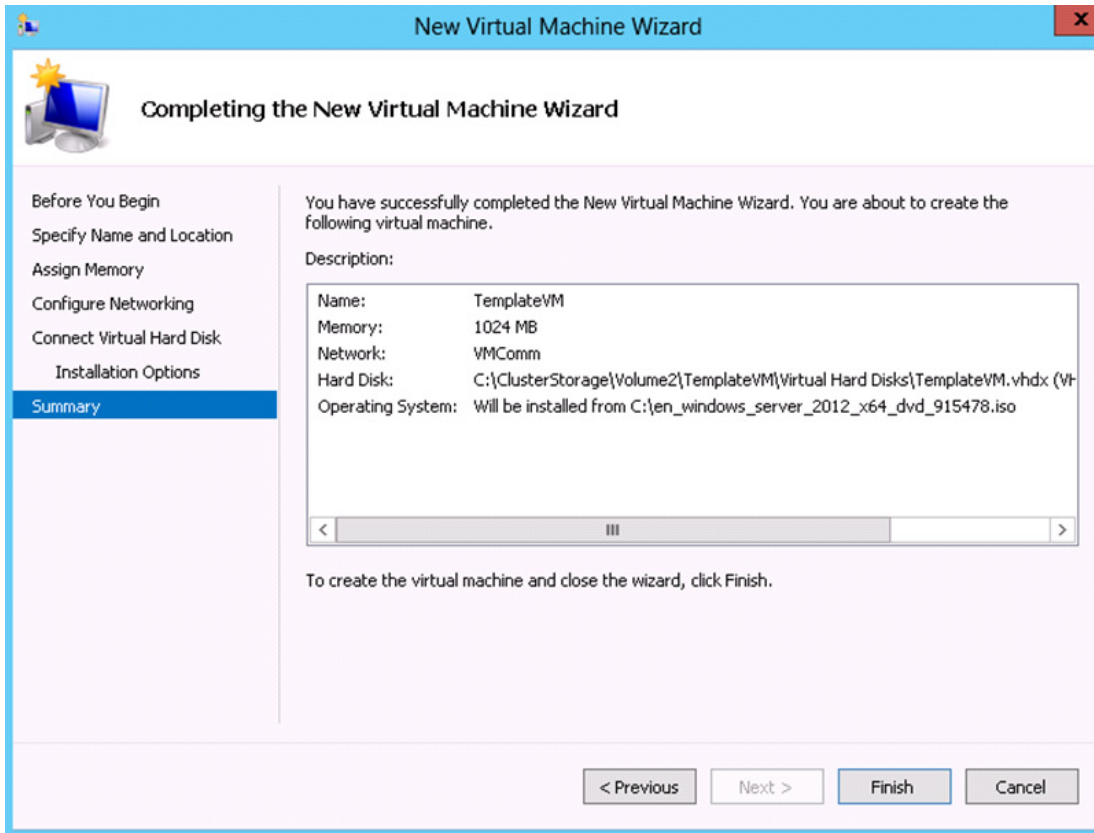
**Figure 131**      *Installation Options in New Virtual Machine Wizard*



16. Review the summary information in the **Completing the New Virtual Machine Wizard** window. If necessary use the **Previous** button to go back to fix any errors.
17. Click **Finish** to create the virtual machine.
18. Click **Finish** on the summary page of the **High Availability Wizard**.



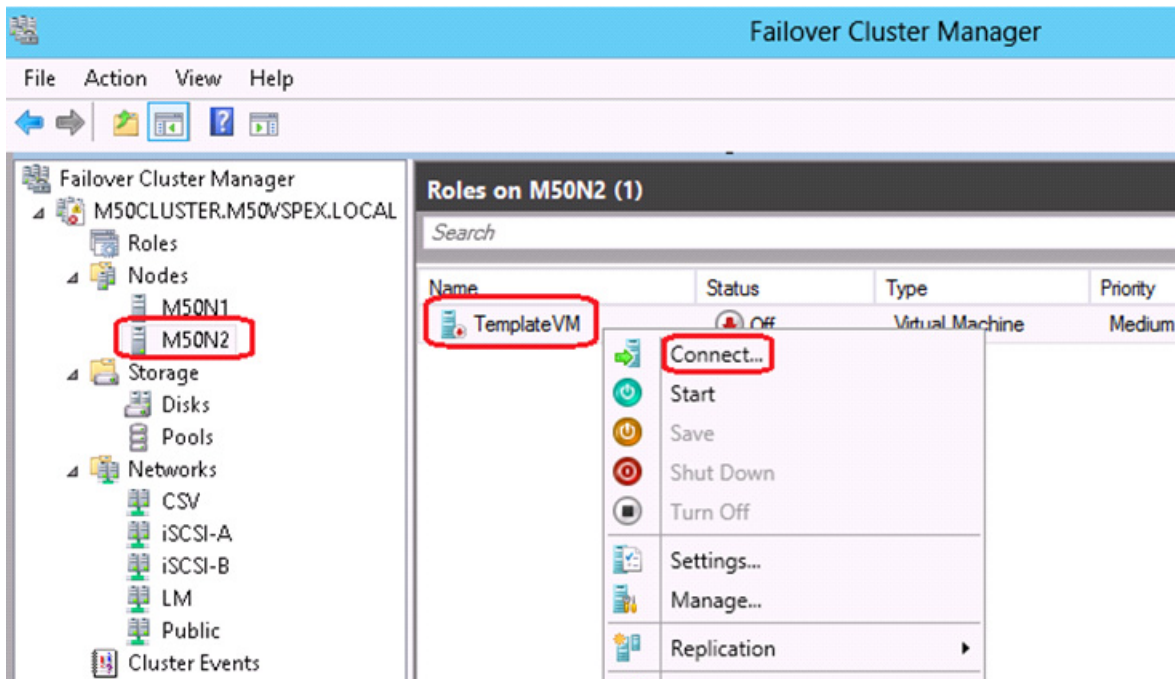
**Figure 132**      *Summary in New Virtual Machine Wizard*



19. Back in **Failover Cluster Manager** expand **Roles**. Right-click on the virtual machine just created and select **Connect...** This brings up a remote connection to the virtual machine.

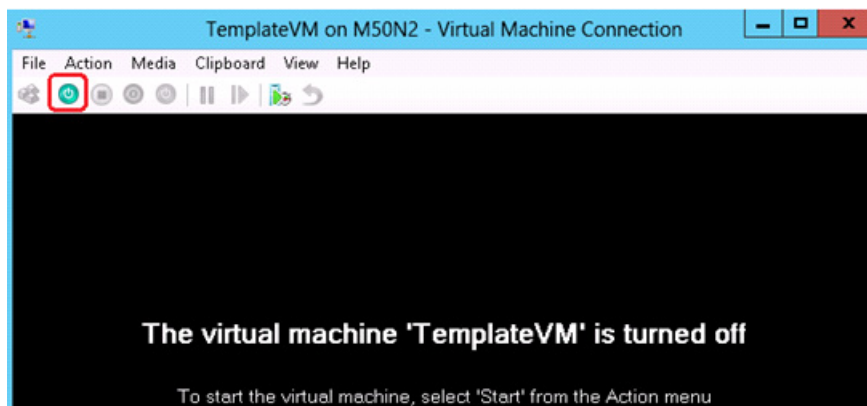


**Figure 133** Roles in Failover Cluster Manager



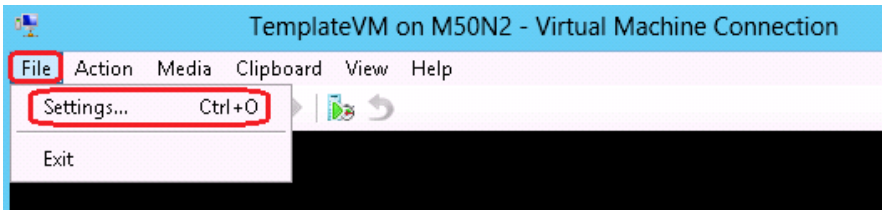
20. Click the **Start** icon to start the virtual machine, which will start the installation process for Windows Server 2012.

**Figure 134** Virtual Machine Connection - Start



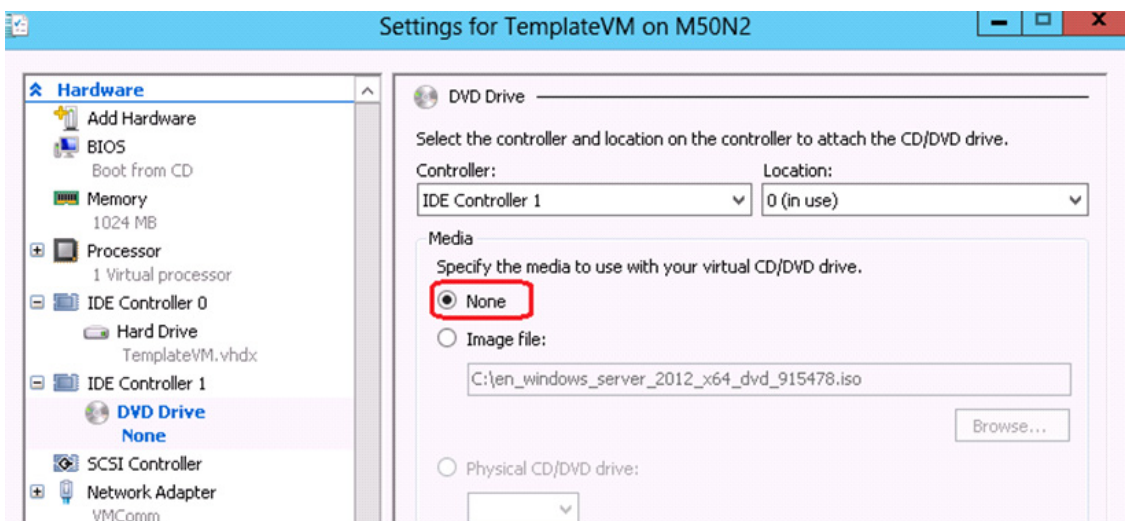
21. Proceed with installing Windows Server 2012, similar to the method followed for installing it on the physical hosts.
22. After completing the installation, remove the installation DVD from the virtual machine. In the **Virtual Machine Connection** window, click **File** and select **Settings...**

Figure 135 Virtual Machine Connection - Settings



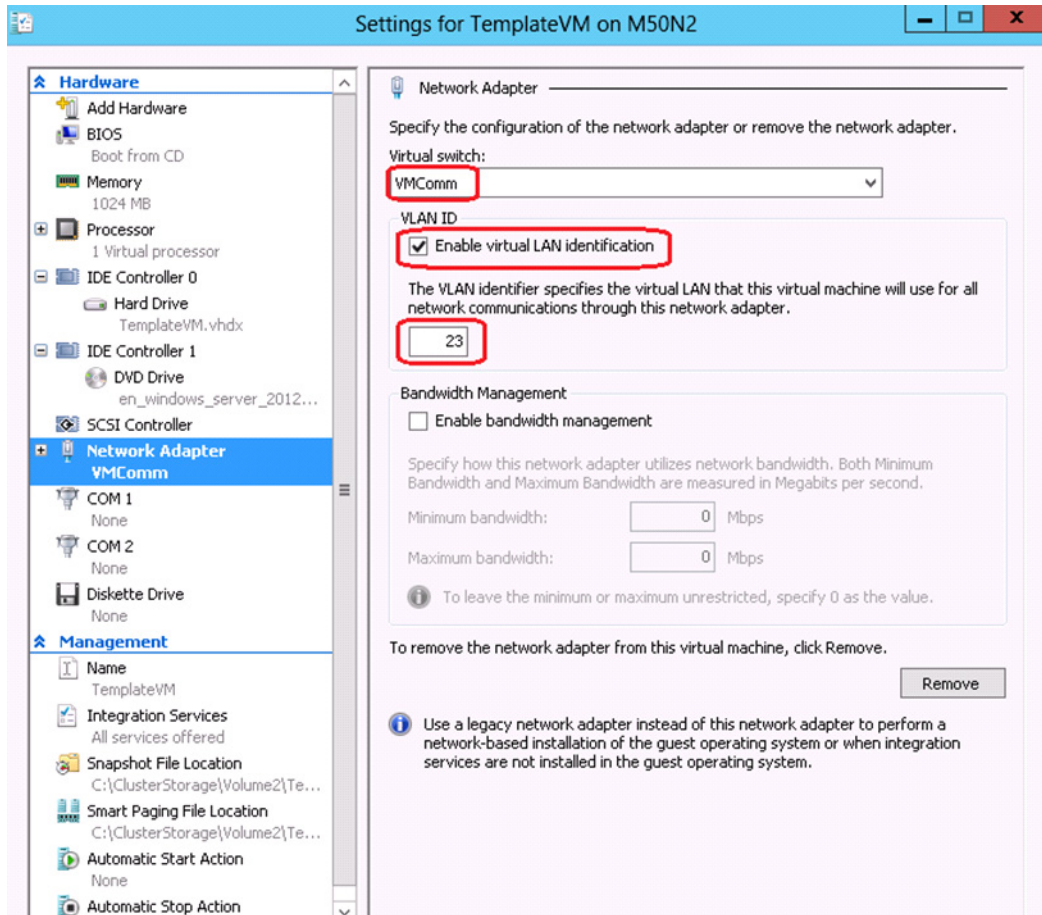
23. In the **Settings** windows, click on the DVD drive. Click the radio button next to **None** and click **OK** to continue.

Figure 136 Virtual Machine Connection – Settings IDE Controller



24. In the **Settings** windows, click on the Network Adapter. Select the check box next to **Enable virtual LAN identification** and specify your **VLAN\_ID** as the VLAN identifier for your VM Traffic.

**Figure 137** Virtual Machine Connection – Network Adapter

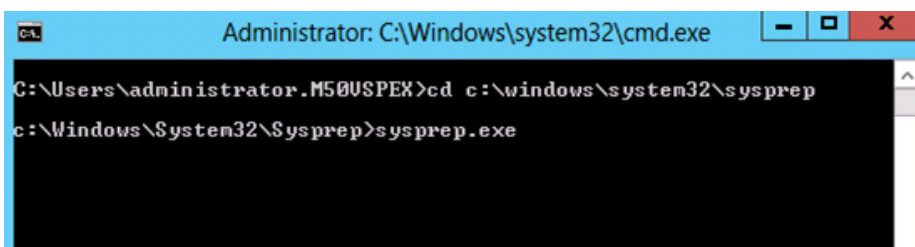


25. Start the VM and customize it as per your standards and requirements. At a minimum, you should ensure all the latest patches have been applied.
26. Once the VM is customized, open command prompt with elevated privileges, connect to `C:\Windows\System32\sysprep` and type `sysprep`.

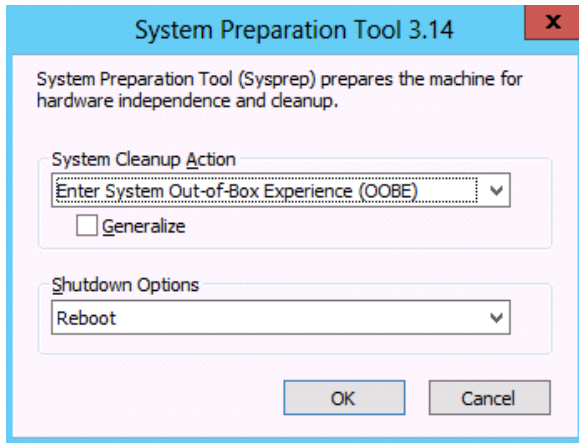


**Note** If working within a PowerShell window, you will need to type `.sysprep.exe`

**Figure 138** Command Prompt - Sysprep



27. In the sysprep tool, check the box for **Generalize**. Select **Shutdown** as the Shutdown Option and click **OK** to continue. Sysprep will prepare the virtual machine for cloning and then power it off.

**Figure 139**      **System Preparation Tool**

28. After this template is created, you can create as many virtual machines as possible by copying the VHDX file and using it as the basis of a new VM.

## Validating Cisco Solution for EMC VSPEX MS Hyper-V Architectures

This section provides a list of items that should be reviewed once the solution has been configured. The goal of this section is to verify the configuration and functionality of specific aspects of the solution, and ensure that the configuration supports core availability requirements.

### Post Install Checklist

The following configuration items are critical to functionality of the solution, and should be verified prior to deployment into production.

1. Move cluster resources from one node another node to check if they migrate successfully.

**Figure 140**      **Validation of Cluster Resources**

```

Administrator: Windows PowerShell
PS C:\Users\administrator.M50VSPEX> Get-ClusterGroup

Name                               OwnerNode      State
----                               -
Available Storage                  M50N1          Online
Cluster Group                     M50N1          Online
TemplateVM                        M50N2          Offline
VM001                             M50N1          Online
VM002                             M50N1          Offline
VM003                             M50N1          Online
VM004                             M50N1          Online
VM005                             M50N1          Online
VM006                             M50N1          Online
VM007                             M50N1          Online
VM008                             M50N1          Online
VM009                             M50N1          Online
VM010                             M50N1          Online
VM011                             M50N1          Online
VM012                             M50N1          Online

PS C:\Users\administrator.M50VSPEX> Move-ClusterGroup "Cluster Group"

Name                               OwnerNode      State
----                               -
Cluster Group                     M50N2          Online

PS C:\Users\administrator.M50VSPEX> Move-ClusterGroup "VM001"

Name                               OwnerNode      State
----                               -
VM001                             M50N2          Online

PS C:\Users\administrator.M50VSPEX>

```

2. Test Live Migration of VMs from one host to other using Failover Cluster Manager.
3. Restart hosts and check if VMs migrate to available hosts
4. Ping with 'do not fragment switch' to validate if jumbo frames are supported end-to-end on storage and live migration VLANs.
5. Deploy a single virtual machine using the Failover Cluster Manager.

Figure 141 Validation of Jumbo Frames support

```

Administrator: Command Prompt
C:\Users\administrator.M50USPEX>ping 10.10.20.11 -f -l 8972

Pinging 10.10.20.11 with 8972 bytes of data:
Reply from 10.10.20.11: bytes=8972 time<1ms TTL=255
Reply from 10.10.20.11: bytes=8972 time<1ms TTL=255
Reply from 10.10.20.11: bytes=8972 time<1ms TTL=255
Reply from 10.10.20.11: bytes=8972 time<1ms TTL=255

Ping statistics for 10.10.20.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\administrator.M50USPEX>ping 10.10.20.12 -f -l 8972

Pinging 10.10.20.12 with 8972 bytes of data:
Reply from 10.10.20.12: bytes=8972 time=1ms TTL=255
Reply from 10.10.20.12: bytes=8972 time=1ms TTL=255
Reply from 10.10.20.12: bytes=8972 time=1ms TTL=255
Reply from 10.10.20.12: bytes=8972 time<1ms TTL=255

Ping statistics for 10.10.20.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\administrator.M50USPEX>hostname
M50N1

C:\Users\administrator.M50USPEX>

```

6. Check if all the port-channels configured in the switch after the host NIC teaming are showing UP status as shown in [Figure 142](#).

Figure 142 Port-Channel Summary

```

N3048A(config-if)# sh port-channel summary
Flags: D - Down      P - Up in port-channel (members)
       I - Individual H - Hot-standby (LACP only)
       s - Suspended  r - Module-removed
       S - Switched   R - Routed
       U - Up (port-channel)

-----
Group Port-  Type  Protocol  Member Ports
Channel
-----
3   Po3(SU)  Eth    LACP     Eth1/3(P)
4   Po4(SU)  Eth    LACP     Eth1/4(P)
5   Po5(SU)  Eth    LACP     Eth1/5(P)
10  Po10(SU)  Eth    LACP     Eth1/51(P) Eth1/52(P)
14  Po14(SU)  Eth    LACP     Eth1/14(P)
16  Po16(SU)  Eth    LACP     Eth1/16(P)
18  Po18(SU)  Eth    LACP     Eth1/18(P)

```



## Verify the Redundancy of the Solution Components

Following redundancy checks were performed at the Cisco lab to verify solution robustness:

1. Administratively shutdown one of the two data links connected to the server. Make sure that connectivity is not affected. Upon administratively enabling the shutdown port, the traffic should be rebalanced. This can be validated by clearing interface counters and showing the counters after forwarding some data from virtual machines on the Nexus switches.
2. Administratively shutdown one of the two data links connected to the storage array. Make sure that storage is still available from all the Hyper-V hosts. Upon administratively enabling the shutdown port, the traffic should be rebalanced.
3. Reboot one of the two Nexus switches while storage and network access from the servers are going on. The switch reboot should not affect the operations of storage and network access from the VMs. Upon rebooting the switch, the network access load should be rebalanced across the two switches.
4. Reboot the active storage processor of the VNXe storage array and make sure that all the iSCSI targets are still accessible during and after the reboot of the storage processor.
5. Fully load all the virtual machines of the solution. Shutdown one of the Hyper-V nodes in the cluster. All the VMs running on that host should be migrated to other active hosts. No VM should lose any network or storage accessibility during or after the migration. Note that in 50 virtual machines architectures, there is enough head room for memory in other servers to accommodate 25 additional virtual machines.

## Cisco validation test profile

“vdbench” testing tool was used with Windows Server 2012 to test scaling of the solution in Cisco labs. [Figure 142](#) provides details on the test profile used.

**Table 12** *VDBench Details*

Profile Characteristics	Value
Number of virtual machines	50
Virtual machine OS	Windows Server 2010
Processors per virtual machine	1
Number of virtual processors per physical CPU core	4
RAM per virtual machine	2 GB
Average storage available for each virtual machine	100 GB
Average IOPS per virtual machines	25 IOPS
Number of datastores to store virtual machine disks	6 CSVs
Disk and RAID type for datastores	RAID 5, 600 GB, 15k rpm, 3.5-inch SAS disks



# Bill of Material

Table 13 gives details of the components used in the CVD for 50 virtual machines configuration.

**Table 13**      **Component Description**

Description	Part #
Cisco UCS C220 M3 rack servers	UCSC-C220-M3S
CPU for Cisco UCS C220 M3 rack servers	UCS-CPU-E5-2650
Memory for Cisco UCS C220 M3 rack servers	UCS-MR-1X082RY-A
RAID local storage for rack servers	UCSC-RAID-11-C220
Broadcom 1Gbps adapter for 50 VMs solution	N2XX-ABPCI03-M3
Cisco Nexus 3048 switches for 50 VMs solution	N3K-C3048TP-1GE
10 Gbps SFP+ multifiber mode	SFP-10G-SR

For more information on the part numbers and options available for customization, see Cisco C220 M3 server specsheet at:

[http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/C220M3\\_SFF\\_SpecSheet.pdf](http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/C220M3_SFF_SpecSheet.pdf)

# Customer Configuration Data Sheet

Before you start the configuration, gather some customer-specific network and host configuration information. Table 14, Table 15, Table 16, Table 17, Table 18, Table 19 provide information on assembling the required network and host address, numbering, and naming information. This worksheet can also be used as a “leave behind” document for future reference.

**Table 14**      **Common Server Information**

Server Name	Purpose	Primary IP
	Domain Controller	
	DNS Primary	
	DNS Secondary	
	DHCP	
	NTP	
	SMTP	
	SNMP	
	vCenter Console	
	SQL Server	

**Table 15**      **Microsoft Hyper-V Server Information**

Server Name	Purpose	Primary IP	Private Net (storage) addresses	
	Microsoft Hyper-V Host 1			
	Microsoft Hyper-V Host 2			
	Microsoft Hyper-V Host 3			

**Table 16**      **Array Information**

Array name	
Admin account	
Management IP	
Storage pool name	
Datastore name	
iSCSI Server IP	

**Table 17**      **Network Infrastructure Information**

Name	Purpose	IP	Subnet Mask	Default Gateway
	Cisco Nexus 3048 Switch A			
	Cisco Nexus 3048 Switch B			

**Table 18**      **VLAN Information**

Name	Network Purpose	VLAN ID	Allowed Subnets
vlan-mgmt	Management and cluster traffic		
vlan-vm_traffic	For VM data traffic		
vlan-iscsi-a	For iSCSI traffic		
vlan-iscsi-b	For iSCSI traffic		
vlan-livemigration	For Live Migration		
vlan-cluster	For CSV and Cluster heart beat		

**Table 19**      **Service Accounts**

Account	Purpose	Password (optional, secure appropriately)
	Microsoft Windows Server administrator	
	Array administrator	

# References

Cisco UCS:

[http://www.cisco.com/en/US/solutions/ns340/ns517/ns224/ns944/unified\\_computing.html](http://www.cisco.com/en/US/solutions/ns340/ns517/ns224/ns944/unified_computing.html)

Cisco UCS C-Series Servers Documentation Roadmap

<http://www.cisco.com/go/unifiedcomputing/c-series-doc>

Cisco Nexus:

[http://www.cisco.com/en/US/products/ps9441/Products\\_Sub\\_Category\\_Home.html](http://www.cisco.com/en/US/products/ps9441/Products_Sub_Category_Home.html)

EMC VNXe3xxx series resources:

<http://www.emc.com/storage/vnx/vnx-series.htm#!resources>

Network Adapter Virtualization Design (Adapter-FEX) with Cisco Nexus 5500 Switches:

[http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9670/guide\\_c07-690080\\_ns1118\\_Networking\\_Solutions\\_White\\_Paper.html](http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9670/guide_c07-690080_ns1118_Networking_Solutions_White_Paper.html)

Configuring Port Channels:

[http://www.cisco.com/en/US/docs/switches/datacenter/sw/5\\_x/dcnm/interfaces/configuration/guide/if\\_portchannel.html](http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/dcnm/interfaces/configuration/guide/if_portchannel.html)

Configuring port-profiles:

[http://www.cisco.com/en/US/docs/switches/datacenter/sw/5\\_x/dcnm/interfaces/configuration/guide/if\\_portprofile.html](http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/dcnm/interfaces/configuration/guide/if_portprofile.html)

Configuring vPCs:

[http://www.cisco.com/en/US/docs/switches/datacenter/sw/5\\_x/dcnm/interfaces/configuration/guide/if\\_vPC.html](http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/dcnm/interfaces/configuration/guide/if_vPC.html)