WHITE PAPER

USING IOMEGA® STORCENTER™ NAS SERVER WITH VMWARE® VSPHERE™ 4

iomega
an EMC company

EMC²

October 2012

EXECUTIVE SUMMARY

VMware® vSphere™ is built on the power of VMware Virtual Infrastructure. This product enables customers to bring the power of cloud computing to their IT infrastructure. VMware ESX Server is a component of vSphere. It is virtual infrastructure software for consolidating and managing systems. ESX Server accelerates service deployments and adds management flexibility by partitioning x86 servers into a pool of secure, portable and hardware-independent virtual machines. VMware vSphere and ESX Server have gained tremendous attraction and acceptance in the industry and are considered critical IT components for enterprises and small businesses alike.

The Iomega® StorCenter™ family of NAS servers are integrated storage devices that offers both NAS and iSCSI functionality to allow customers flexible deployment options. The product targets small- to medium-sized businesses with a rich set of features and simplicity of management. The Iomega StorCenter NAS servers are powered by EMC LifeLine software to allow businesses to protect and share data with EMC's world class storage and security technologies.

This white paper examines how an Iomega StorCenter NAS server can be used to present storage to VMware ESX Server in a virtual environment. The paper also provides detailed procedures that illustrate how to create storage on an Iomega StorCenter NAS server in different forms and then utilize the storage on a VMware ESX Server

INTRODUCTION

VMware ESX Server supports NAS devices using the NFS and iSCSI protocols. Iomega StorCenter NAS servers can present NFS-exported shares and iSCSI LUNs to VMware ESX Server to create Datastores for virtual machines and virtual disks. An Iomega StorCenter NAS offers greater reliability, ease of use, and ease of management characteristics that are designed specifically for the needs of small- to medium-sized businesses.

VMware ESX Server can connect to iSCSI targets using either software or hardware iSCSI initiators. The LUNs presented by a target can then be formatted in the proprietary VMFS format. VMware ESX can also use iSCSI LUNs in the form of RDM to provide direct raw disk access to virtual machines. VMFS is the native storage option on VMware ESX Server, It's also how SAN storage and local disks are utilized to create datastores.

NFS is another compelling option for VMware ESX for many reasons. With NFS, VMware ESX Server supports advanced features including VMotion, Distributed Resource Scheduler (DRS), high availability (VMHA), and VMware Consolidated Backup (VCB). NFS offers a highly simplified management model that reduces cost and management complexity. VMware encapsulates virtual machines into a small number of .vmdk files. NFS is an optimized file-serving protocol with operational granularity at the file level as opposed to the LUN level.

Iomega StorCenter NAS satisfies requirements for both storage options on VMware ESX Server and is certified in the VMware Hardware Compatibility List (HCL) with certifications in both NAS and Software iSCSI categories. A StorCenter NAS device is a proven storage platform for small businesses that want to deploy VMware vSphere

AUDIENCE

Information contained in this white paper is intended for Iomega customers, partners, and service personnel involved in planning, architecting, or administering a VMware environment with an Iomega StorCenter NAS as the storage device. The readers are expected to have experience with VMware ESX Server and an Iomega StorCenter NAS device that runs EMC LifeLine software.

TERMINOLOGY

- **Datastore**: A file system, either VMFS or NFS, that serves as a virtual representation of an underlying pool of physical storage resources. These physical storage resources can be comprised of SCSI disks from a local server, Fibre Channel SAN disk arrays, iSCSI SAN disk arrays, or NAS storage arrays.

iomega
an EMC company

- **Internet SCSI (iSCSI)**: A protocol for sending SCSI packets over TCP/IP networks
- **iSCSI LUN**: iSCSI LUN (Logical Unit Number) is a virtual disk that processes SCSI commands, such as reading from and writing to storage media.
- **Network File System (NFS)**: A distributed file system providing transparent access to remote file systems. NFS allows all network systems to share a single copy of a directory.
- **Raw Device Mapping (RDM)**: RDM includes a combination of a pointer, which is a .vmdk file that resides on a VMFS volume, and a physical raw device that the .vmdk file points to. RDM can either be physical compatibility mode or virtual compatibility mode.
- **Virtual Machine**: A virtualized x86 PC on which a guest operating system and an associated application run. A VM is also a set of discrete files that primarily include a .vmx configuration file and one or more .vmdk virtual disk files.
- **Virtual Machine File System (VMFS)**: A VMware proprietary file system installed onto data stores and used by ESX Server to house virtual machines.
- **CHAP**: Challenge Handshake Authentication Protocol. Access control protocol for secure authentication using shared passwords called secrets.
- **iSNS**: Internet Storage Name Service. Discovery and naming protocol designed to facilitate the automated discovery, management, and configuration of iSCSI and Fibre Channel Protocol (FCP) devices on a TCP/IP network.
- **NIC teaming**: a computer networking technology that uses multiple network ports/cables in parallel to increase the link speed beyond the limits of any one single port/cable and to increase the redundancy for higher availability. Other similar terms include NIC bonding, link aggregation, Ethernet trunk, etcs.
- **iSCSI session**: a session is a relationship between an initiator node and a target node. It is identified by initiator session identifier assigned by initiator and made known to target during login. A session requires an iSCSI connection to be established, and may have more than one iSCSI connections assigned to it.
- **iSCSI target**: iSCSI endpoint, identified by a unique iSCSI name, which executes commands issued by the iSCSI initiator.
- **iSCSI initiator**: iSCSI endpoint, , identified by a unique iSCSI name, which begins an iSCSI session by issuing a command to the other endpoint (the target).

SOLUTION CONFIGURATION

This section lists hardware and software resources for provisioning the StorCenter px6-300d storage device to VMware ESX Server 4, as illustrated in this white paper.

HARDWARE

Table 1 lists the hardware resources used in the testing environment for the paper.

Hardware	Quantity	Configuration
Iomega® StorCenter™ px6-300d NAS Server	one	Intel Atom Dual Core, 1.8GHz CPU 2 GB memory Six 2 TB (7200 rpm) SATA disks RAID 5 across the disks Dual GbE network connections
Dell PowerEdge 1850	one	Two Intel Xeon 3.00GHz CPUs 8 GB of memory One 146 GB 15k internal SCSI disk Four 10/100/1000 MB Ethernet NICs

Table 1 Hardware resources

SOFTWARE

Table 2 lists the software resources used in the testing environment for the paper.

Software	Quantity	Configuration
EMC® LifeLine™ 3	one	EMC firmware that runs the Iomega StorCenter px6-300d NAS device
VMware ESX Server 4.1	one	Installed on a Dell PowerEdge 1850 machine
VMware vCenter Server 4	one	Installed on a Windows host for vSphere management

Table 2 Software resources

DEPLOYMENT ROADMAP

Following its installation and initial configuration, the ESX Server can be connected to shared storage that is presented from the StorCenter px6-300d over the NFS and the iSCSI network protocols. Figure 1 highlights the steps that should be followed when connecting the StorCenter px6-300d storage device to the ESX Server.

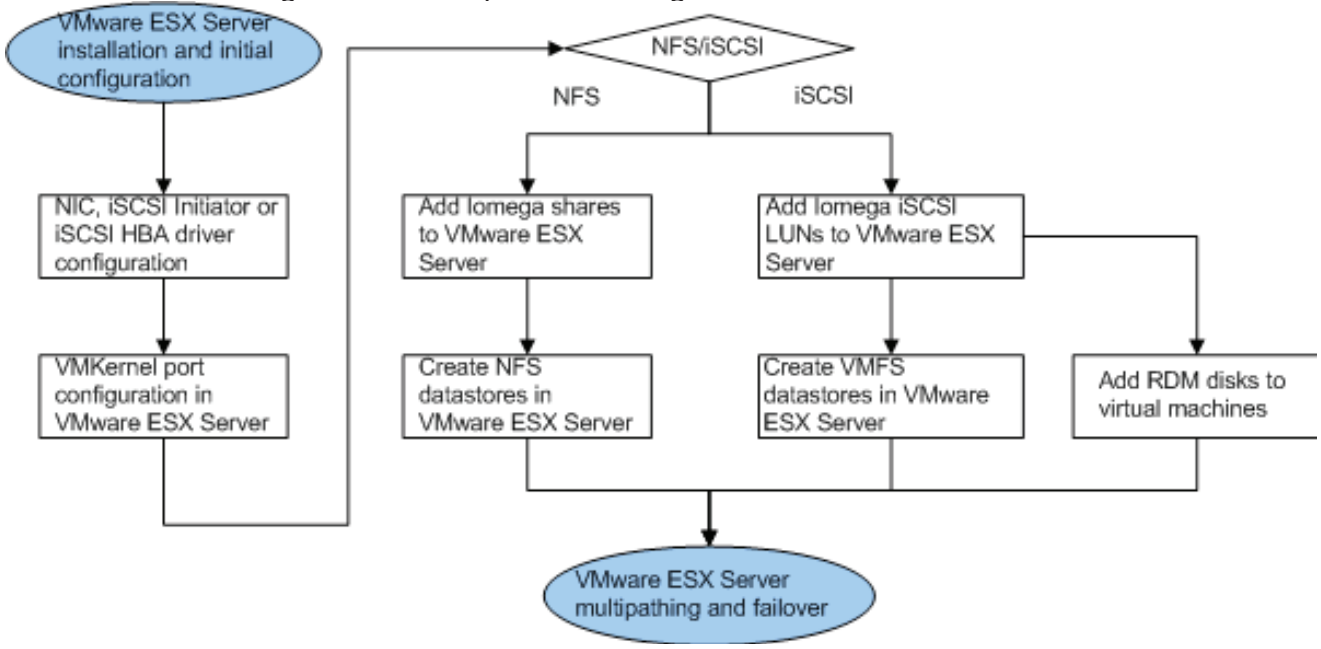


Figure 1 High-level roadmap for connecting the ESX Server to a StorCenter NAS

This white paper provides further information on each of these steps as follows:

- NIC and iSCSI initiator configuration in the ESX Server – configuring the physical NIC, software iSCSI initiator or the iSCSI HBA that will be used to connect the ESX Server to an StorCenter NAS.
- VMkernel port configuration in the ESX Server – configuring the ESX Server for IP storage connections to a StorCenter NAS for both the NFS and iSCSI network storage protocols.
- Adding Iomega shares to the ESX Server – for NFS, creating and exporting Iomega shares to the ESX Server.
- Creating NFS datastores in the ESX Server – for NFS, configuring NFS datastores in the ESX Server on the exported shares from a StorCenter NAS.

- **Adding iSCSI LUNs to the ESX Server** – for iSCSI, creating and sharing Iomega iSCSI LUNs to the ESX Server.
- **Creating VMFS datastores in the ESX Server** – for iSCSI, configuring VMFS datastores over the iSCSI LUNs that were provisioned from a StorCenter NAS.
- **Adding RDM disks to virtual machines** – for iSCSI, alternatively making the LUNs available as RDM disks to the virtual machines.
- **Multipathing and failover in the ESX Server** – best practices for designing highly available network architecture in the ESX Server.

NIC AND ISCSI INITIATOR CONFIGURATION

The NIC and iSCSI HBA drivers provided by VMware as part of the ESX Server distribution should be utilized when connecting the ESX Server to a StorCenter NAS device.

For iSCSI, both the ESX Server software iSCSI initiator and an iSCSI HBA can be used to connect to StorCenter NAS iSCSI targets. When using iSCSI HBA, please refer to the VMware I/O Compatibility Guide (http://www.vmware.com/resources/compatibility/pdf/vi_io_guide.pdf) for a list of supported HBAs.

VMKERNEL PORT CONFIGURATION

A VMkernel port allows for the usage of both iSCSI and NFS storage. When the storage has been configured on a StorCenter NAS, the ESX server host must have a VMkernel port defined with network access to the Iomega device.

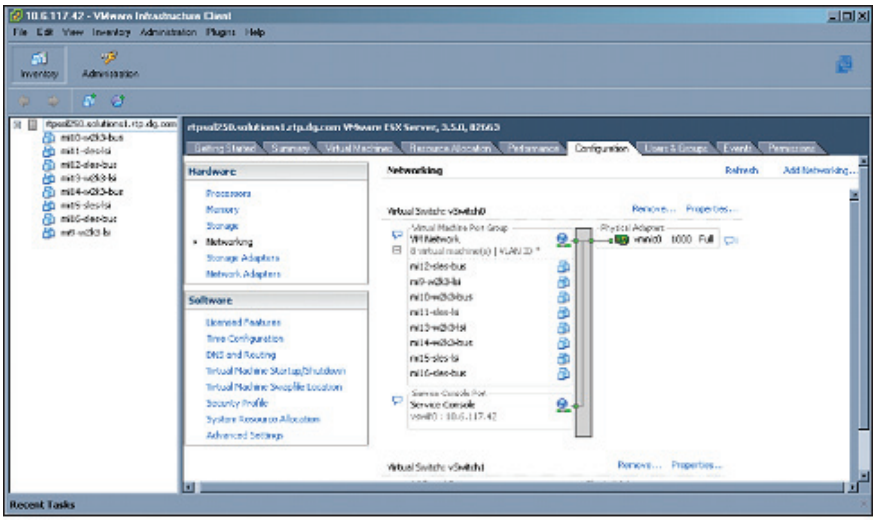
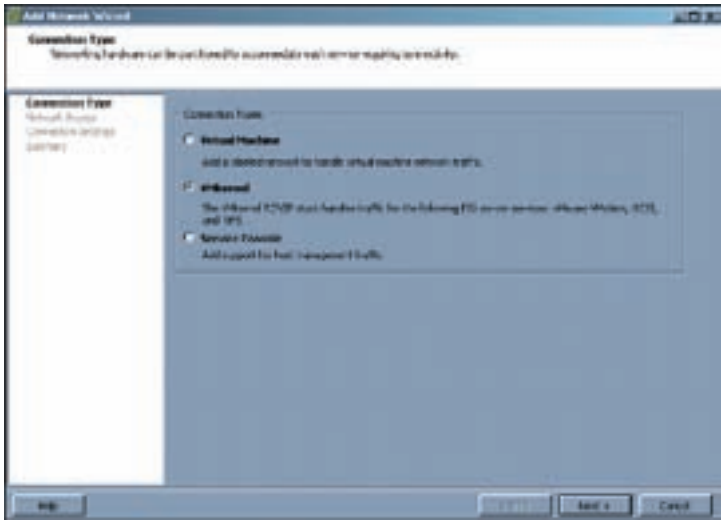
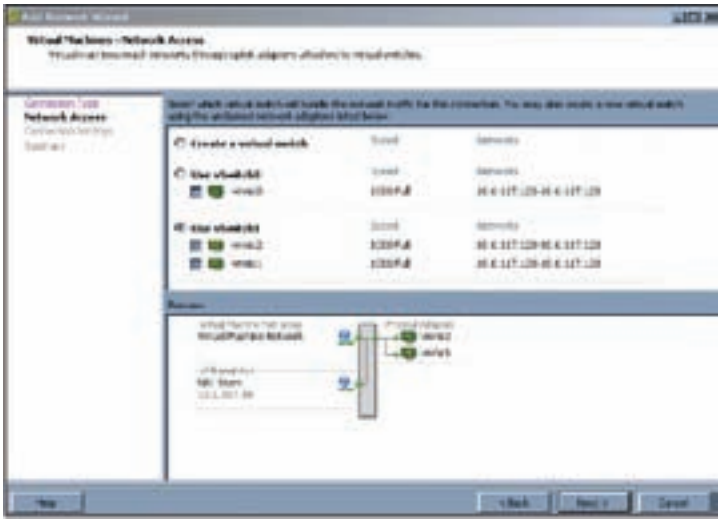
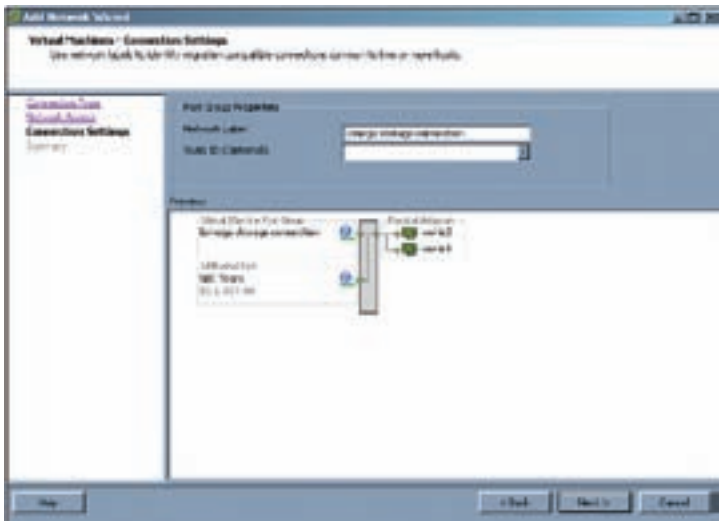


Figure 2 Add network

1. Click **Configuration › Networking › Add Networking.**







2. Select the VMkernel connection type as shown in Figure 3.

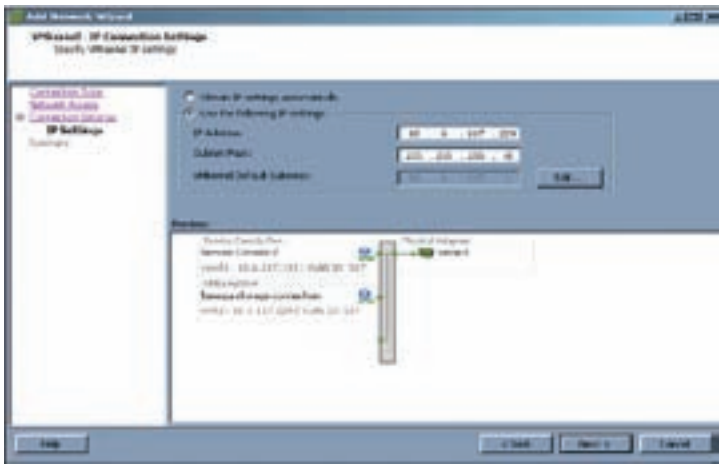


Figure 3 VMkernel selection

3. Select a virtual switch to handle the VMkernel port traffic.

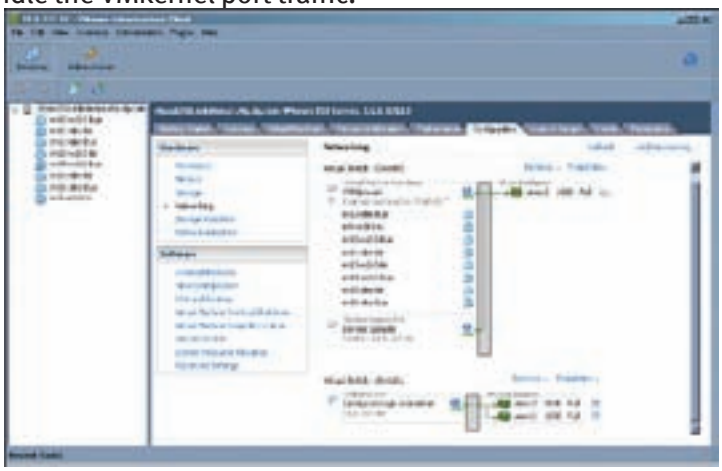


Figure 4 Select virtual switch

4. Name the new VMkernel port group and optionally the VLAN ID for the network.

Figure 5 Name the VMkernel port group

5. Configure IP settings on the VMkernel port.

Figure 6 Configure IP settings for the port

6. Verify the settings and finish creating the VMkernel port.

Figure 7 VMkernel port group created

ADDING A SHARE ON AN IOMEGA STORCENTER NAS DEVICE

When using NFS storage, you need to add a share on the StorCenter NAS device. Appropriate access permissions must be set for the VMkernel port on the ESX Server to mount an NFS share. These access permissions are:
Host access – provide the VMkernel port mount access to the share.
Read/write access – provide the VMkernel port read/write access to the share.
Root access – provide the VMkernel port root access to the share.

There are settings on NFS exported shares on the StorCenter NAS. Do not use “root_squash”. This means that root on the client machine will be mapped to the anonymous UID, which is commonly nobody. The result is that root on the client machine will not be able to access anything in the exported entry. The no_root_squash option prevents

this behavior. Therefore, if you want to secure the share to be used by ESX, you must enable root account access on your StorCenter NAS. If you choose to leave the share non- secured, then nothing special needs to be done.

1. On **Network › Protocols** click the switch to turn on NFS. The “NFS Settings” window appears. Please verify, that

“Allow all client users full access” is selected, if you intend to secure the NFS share so that the ESX server can access it using the default root account. Click “Apply” to complete the activation of NFS.

Figure 8 Enable NFS service on StorCenter NAS

2. To create a new share goto **Storage › Shares** and click on “Add a Share”. Type in the name of the new share, make sure “Media sharing” is not ticked, and click “Create”.

Figure 9 Create a new share

3. Click “Access Permissions” to open the tab to specify user access to the secured share.

Figure 10 Specify user access

4. The “NFS” tab is to set NFS host access security on the share. Make sure you enter the IP address of the VMKernel port created previously, not the service console port.

Figure 11 Specify host access

5. Click Apply. The ”Information” tab of the created share should look like this:

Figure 12 New share created

CREATING AN NFS DATASTORE ON ESX SERVER

VMware Infrastructure 3 management utilities are used to configure and mount NFS shares from the Iomega StorCenter NAS. The VI client is also used to assign a datastore name to the export. The datastore name is the key reference that is used to manage the datastore within the ESX environment.

The NFS datastore is viewed as a pool of storage space to support virtual disks. One or more virtual disks are created within the datastore and assigned to virtual machines. Each virtual machine will use the primary virtual disk to install the guest operating system and boot information. The additional disks are used to support application and user data.

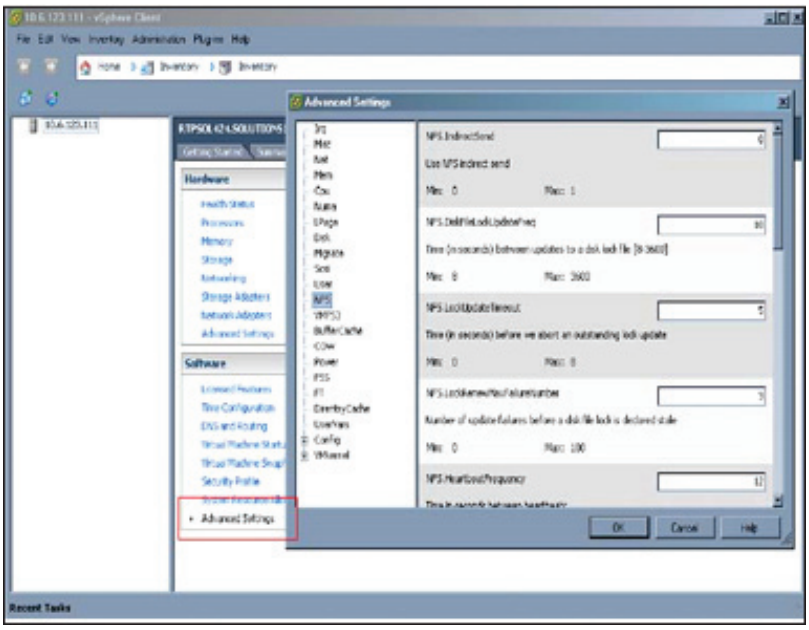
By default, the ESX Server allows a maximum of eight NFS datastores to be created. To create more NFS datastores, please change the NFS.MaxVolumes setting to a number no greater than 32. The following settings are

recommended for NFS connections:

NFS.MaxVolumes = 32

NFS.HeartbeatFrequency = 12

NFS.HeartbeatTimeout = 5

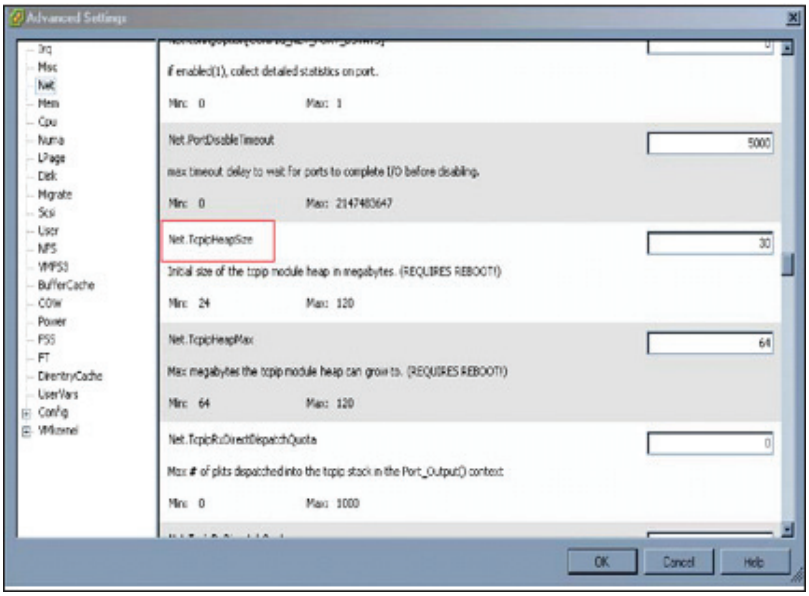


NFS.HeartbeatMaxFailures = 10

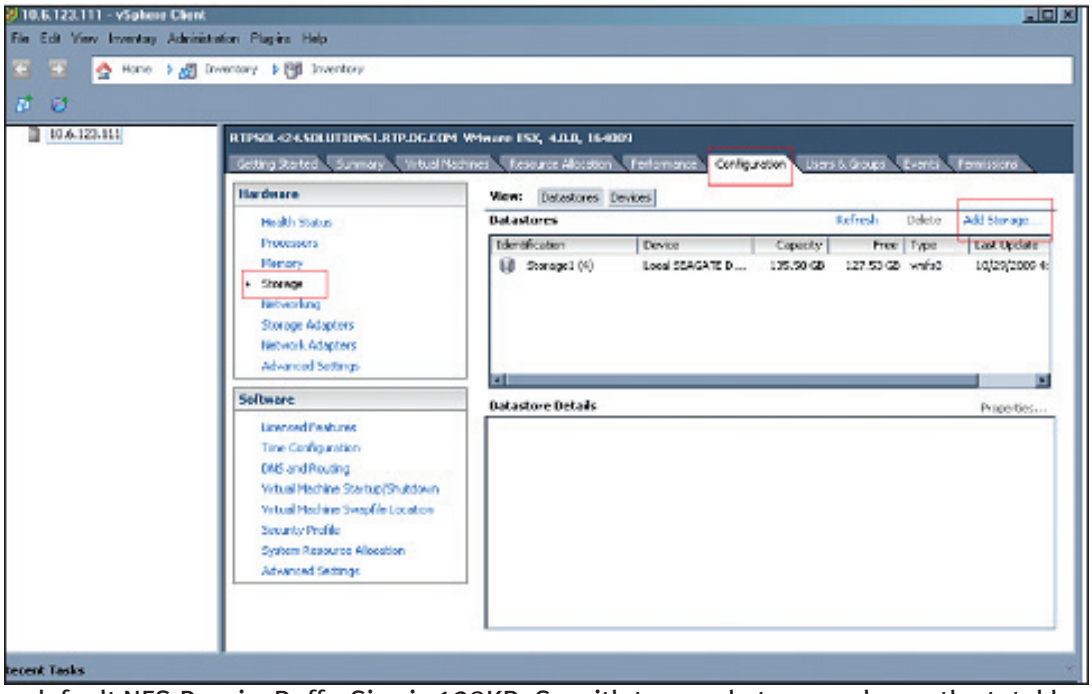
Net.TcpipHeapSize = 30

The three heartbeat options control heartbeat counts and timeouts. In the event of a brief network connection loss, reboot, or failure of the NFS server, the ESX Server will not simply fail the NFS datastores. The NFS client in ESX relies on heartbeats to verify the NFS shares are available. Therefore, increasing the NFS heartbeat frequency will ensure the NFS datastore I/O can resume much sooner, once the NFS server comes back.

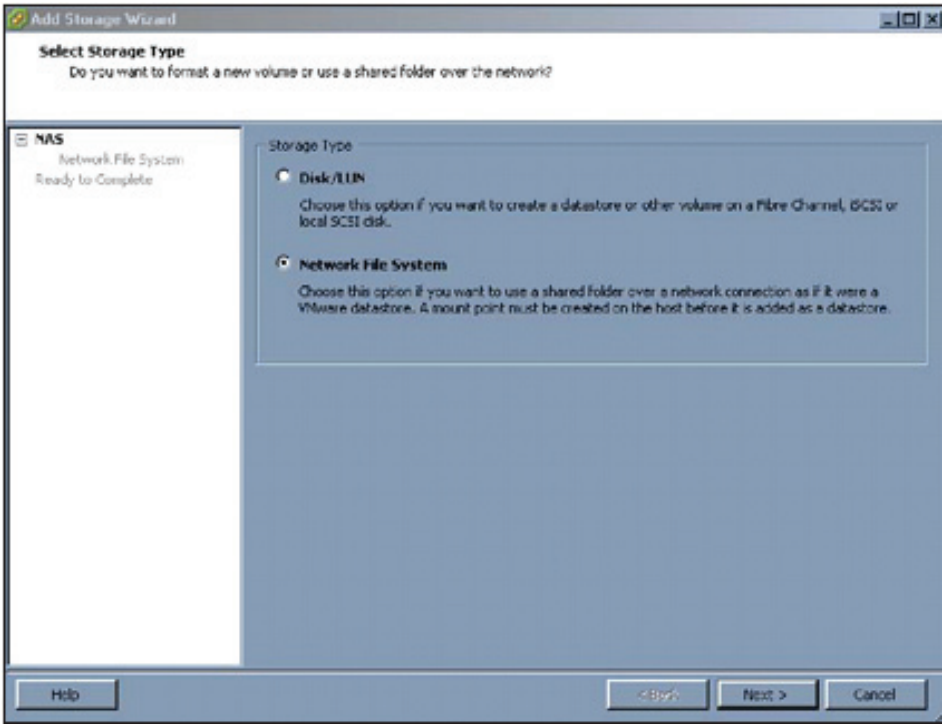
Figure 13 Modify NFS options on ESX Server



The TCP/IP heap is memory used for TCP/IP buffers for NFS, iSCSI, VMotion, etc. The default NFS.SendBufferSize

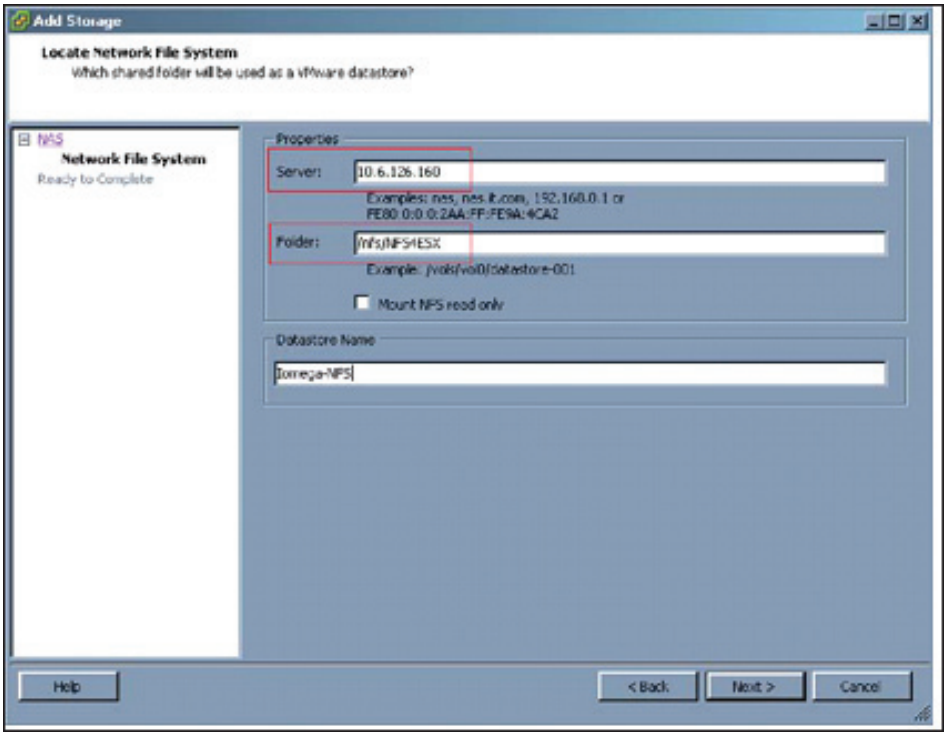


is 264KB, and the default NFS.ReceiveBufferSize is 128KB. So with two sockets per volume, the total heap needed per volume is 784KB. If you want to create a total of 32 NFS datastores, then you need approximately 25MB in heap size. If you set the heap size to 30MB, you will ensure the best NFS datastore performance when the maximum



number of datastores are created.

Figure 14 Modify TCP/IP heap size



1. Go to **Configuration › Storage › Add Storage...**

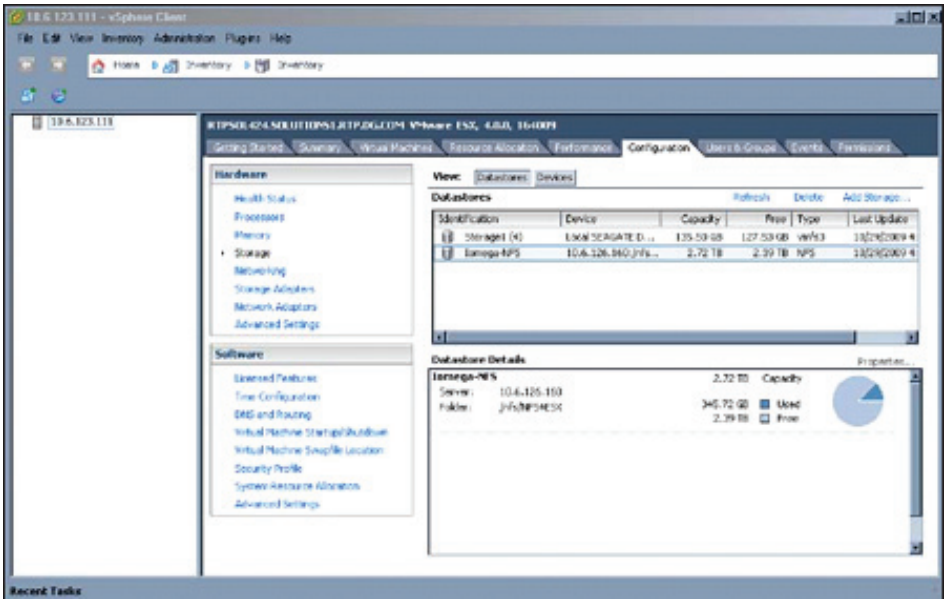
Figure 15 Add storage to ESX Server

2. Select the **Network File System** option.

Figure 16 Select NFS type

3. Enter the NFS server and share information of the StorCenter NAS.

Figure 17 Mount the NFS share



Either the hostname or the IP address of the StorCenter NAS can be entered here. Ensure that "/nfs" is specified in the folder path so Lifeline can export an NFS share. A meaningful datastore name is recommended to clearly identify it in ESX Server.

4. Click Next and confirm the settings to create the datastore.

Figure 18 Create NFS datastore

ADDING AN ISCSI LUN ON AN IOMEGA STORCENTER NAS DEVICE

When using iSCSI storage, you need to add an iSCSI LUN on a StorCenter NAS. You create an iSCSI target on the StorCenter NAS, which is holding one single LUN. An iSCSI LUN can be protected by setting user access controls and iSCSI authentication methods.

The StorCenter NAS server supports two methods of target discovery: the SendTargets command, and the Internet Storage Name Service (iSNS) server. The SendTargets command technique requires that an iSCSI initiator knows the IP address and port number of the target. It is the simple and default discovery method. The VMware ESX Server only supports SendTargets; therefore, this is the discovery method used.

After target discovery, an iSCSI initiator can log on with or without authentication. The StorCenter NAS supports the CHAP authentication method. When CHAP is enabled and an iSCSI LUN is secured, an initiator will need to provide

the CHAP secret to log on. However, if the LUN is not secured, no authentication is required even if the global CHAP setting is enabled. Iomega customers are recommended to secure iSCSI LUNs, and this is the practice followed in the white paper.

1. On **Storage › iSCSI** click the switch to turn on iSCSI . Optionally iSNS discovery and two-way authentication can be enabled by clicking on **Settings**.

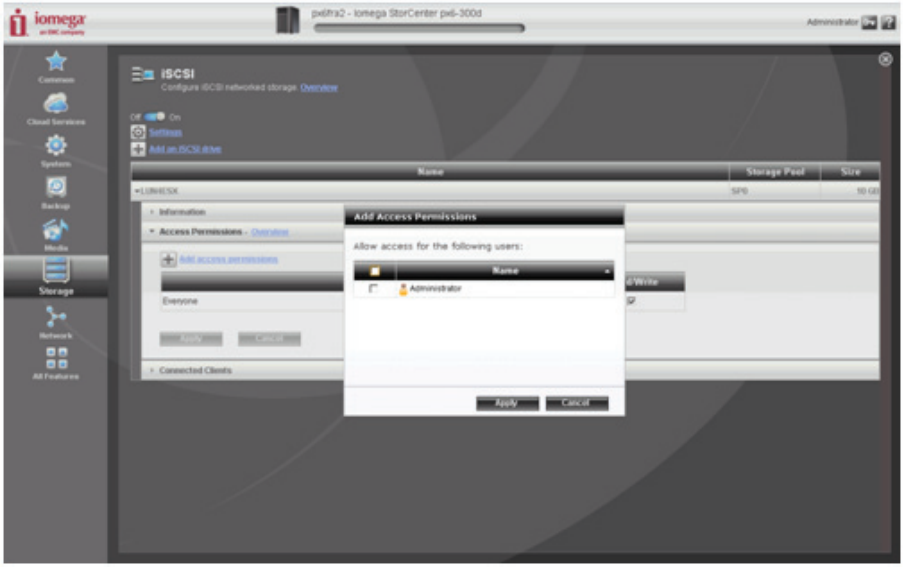


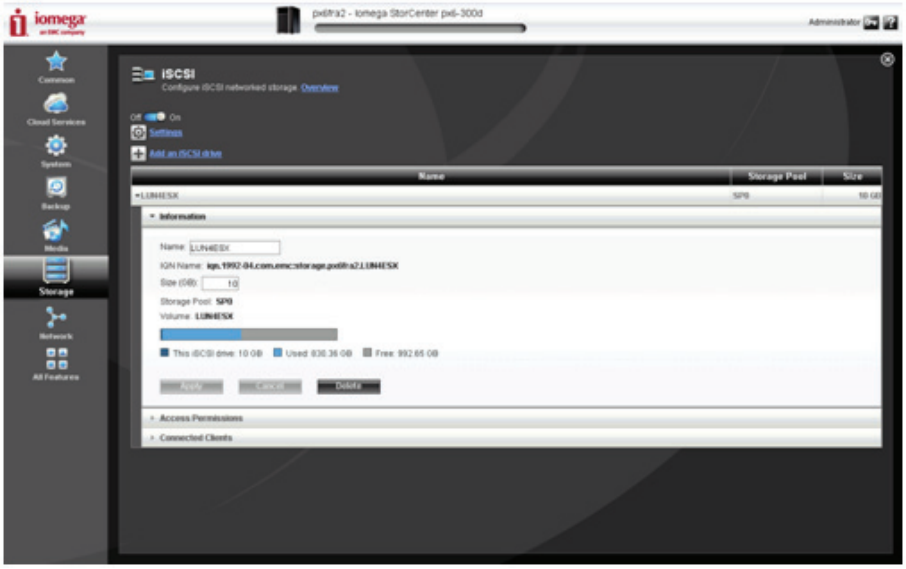
Figure 19 Enable iSCSI service

2. Click on “Add an iSCSI drive”. Type in the name and size of the iSCSI drive and click “Create”.

Figure 20 Add new LUN

3. Click “Access Permissions” to open the tab to specify user access to the iSCSI drive. To enable security click on “Add access permissions”, select the user und click “Apply”.

Figure 21 Set user access to the LUN

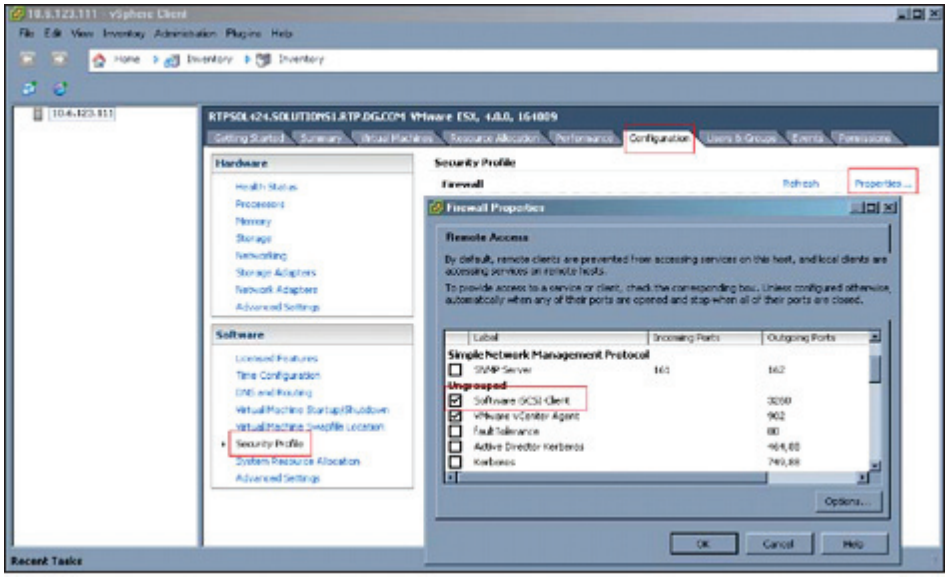


In this example, the user account *Administrator* is given read/write access to the LUN, but other users have no access to it. This Administrator user account and its password will be the CHAP logon credentials to be used by ESX Server.

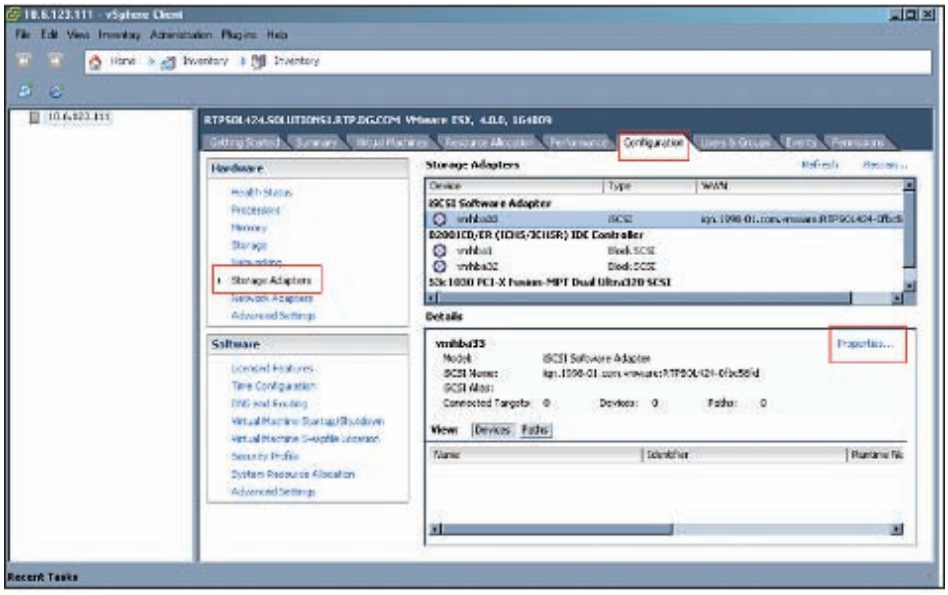
4. The ”Information” tab of the created iSCSI LUN should look like this:

Figure 22 Information of the LUN creation

CREATING A VMFS DATASTORE ON THE ESX SERVER



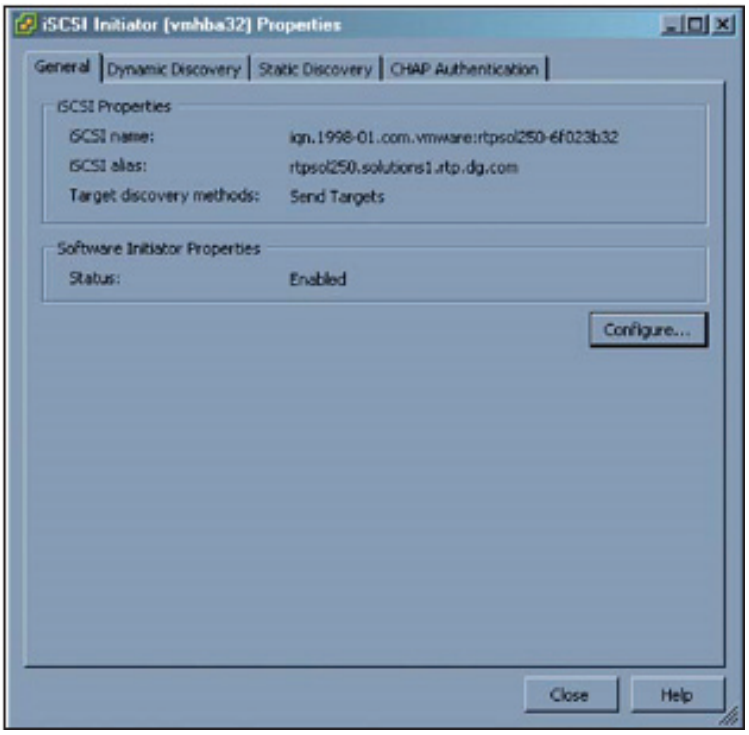
Prior to adding an iSCSI device on the ESX Server, an iSCSI initiator must be installed. Two types of initiators, software and hardware, can be used in the ESX Server. Each type has a distinct installation method. After installation, however, both initiators use the same process to discover targets, log on to the targets, scan for new

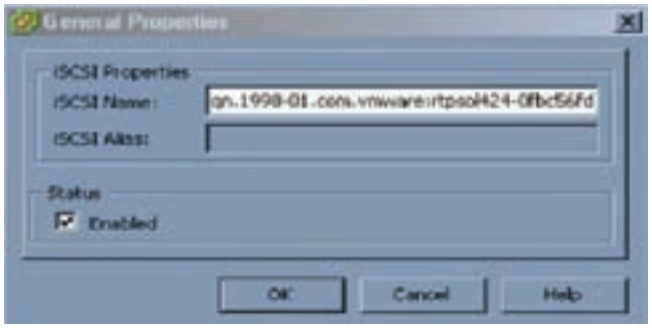


iSCSI LUNs, and create VMFS datastores using those LUNs. In this white paper, the software iSCSI initiator is used to illustrate the process.

1. Enable the iSCSI client in the VMware ESX firewall. Go to **Configuration › Security Profile › Properties...**

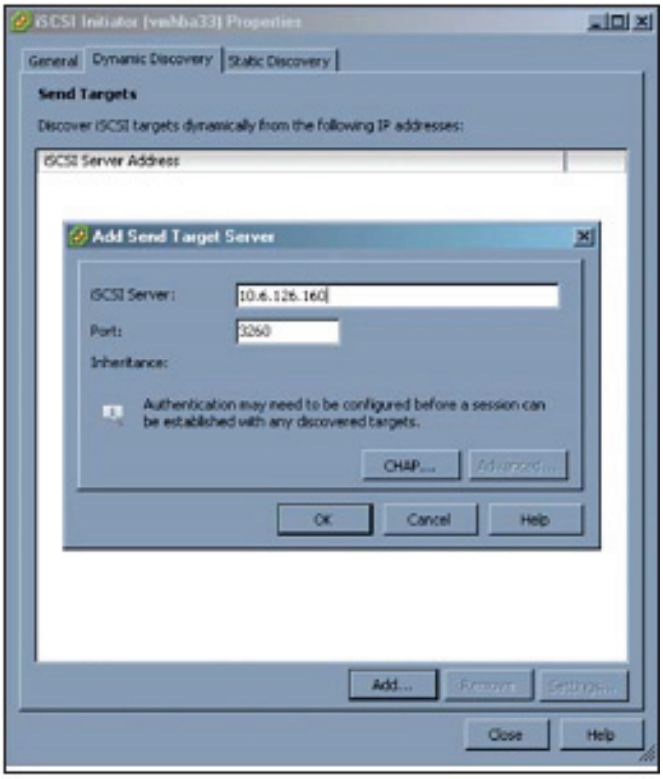
Figure 23 Enable iSCSI client





2. Click **Configuration › Storage Adapters**

Figure 24 iSCSI Software Adapter



3. Click the **vmnba32** iSCSI software adapter and then click **Properties.** If the iSCSI initiator is not enabled yet, click

Configure to enable the initiator and use the default iSCSI name.

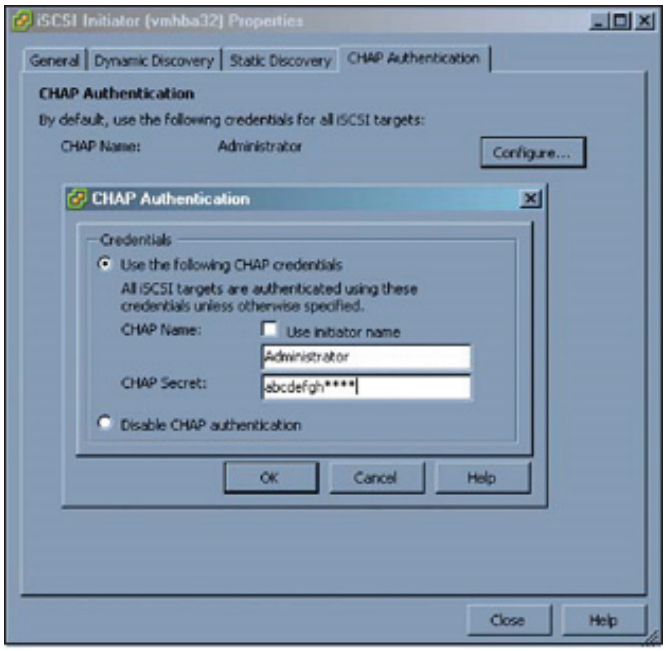


Figure 25 iSCSI initiator properties

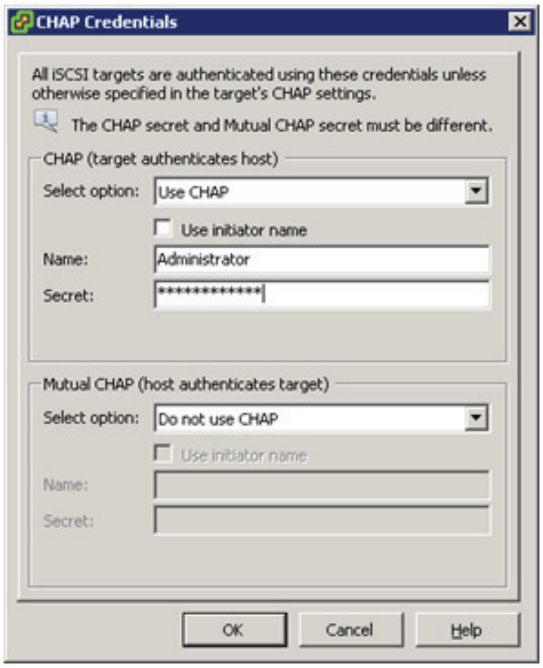
4. Click **Dynamic Discovery › Add** to enter the iSCSI server information. As mentioned previously, the SendTargets discovery method is used.

Figure 26 Specify iSCSI server information

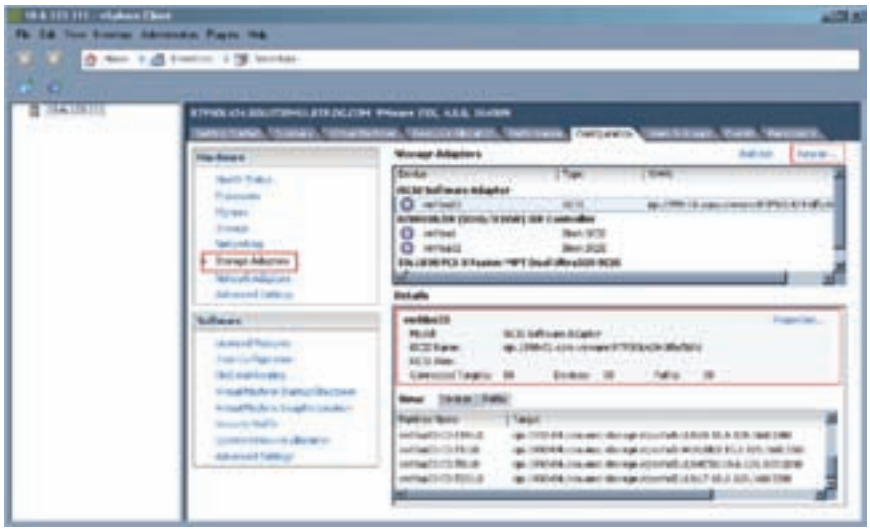
5. The iSCSI server should be added successfully.

Figure 27 List iSCSI server

6. Go back to the General tab. Click CHAP to enter the CHAP authentication credentials for logon to the iSCSI targets on the StorCenter NAS.



7. Select “Use Chap” from “Select option” in the CHAP pane. The CHAP name should be the user name that is granted read/write access to an iSCSI LUN. In this example, it’s Administrator. The CHAP secret is the password

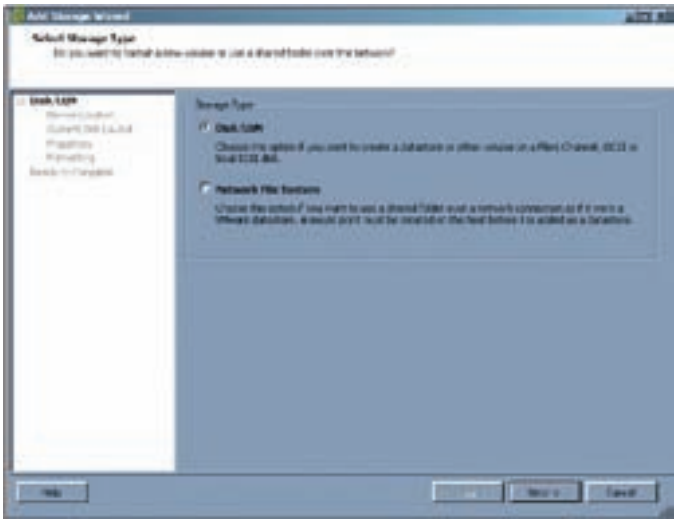


of the user account as set on the StorCenter NAS. A CHAP secret is required to have 12-16 characters if IPSec is not used. Therefore, if the user password is shorter than 12 characters, increase its length with the asterisk * character. In this example, the password is abcdefgh, so the CHAP secret is abcdefgh****.

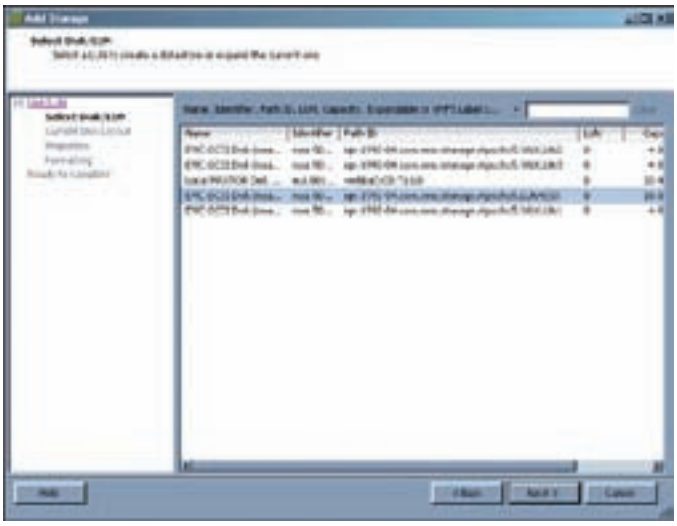
Figure 28 Supply CHAP authentication information

8. Go to **Configuration › Storage Adapters** and click “Rescan All…” to discover targets and LUNs on the StorCenter NAS.

Figure 29 Target and LUN discovery



All the targets and LUNs that are either unsecured or granted access to the admin user display as disks in the VMware ESX.



9. Go to **Configuration › Storage › Add Storage…** again to create VMFS datastore.

10. Select the Disk/LUN option.

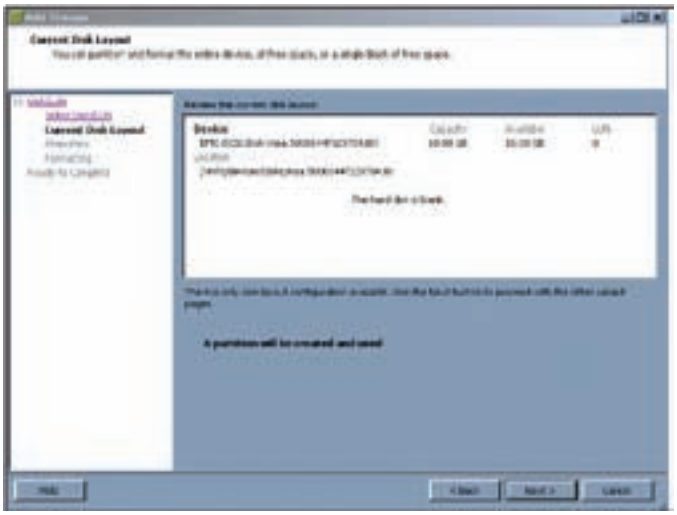


Figure 30 Select the VMS type

11. Select the iSCSI LUN to create VMFS on.

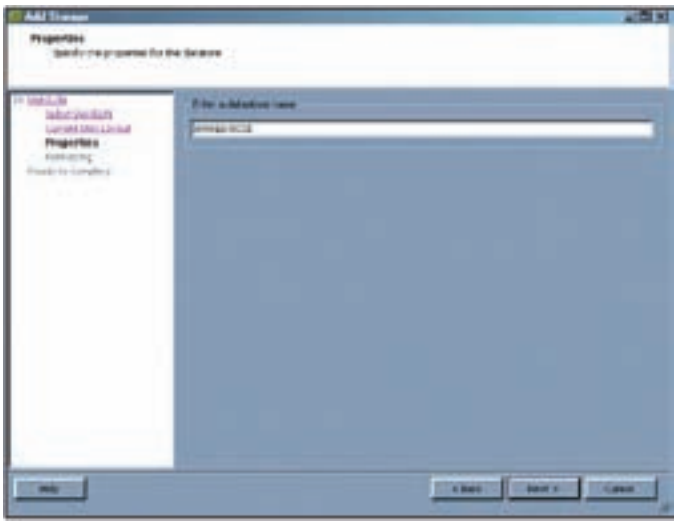
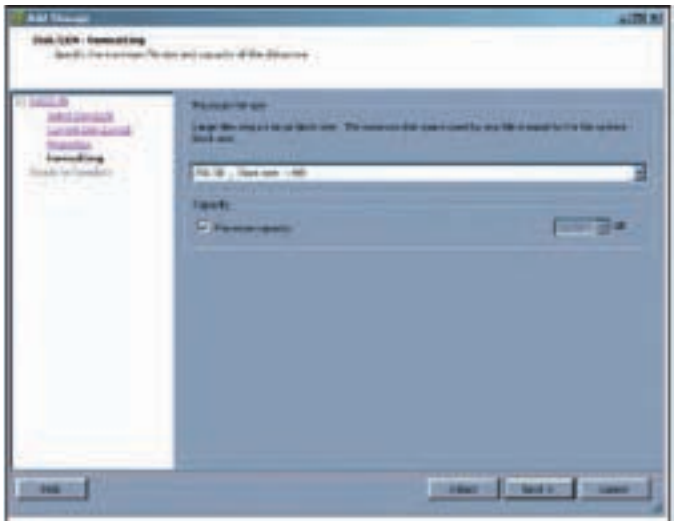
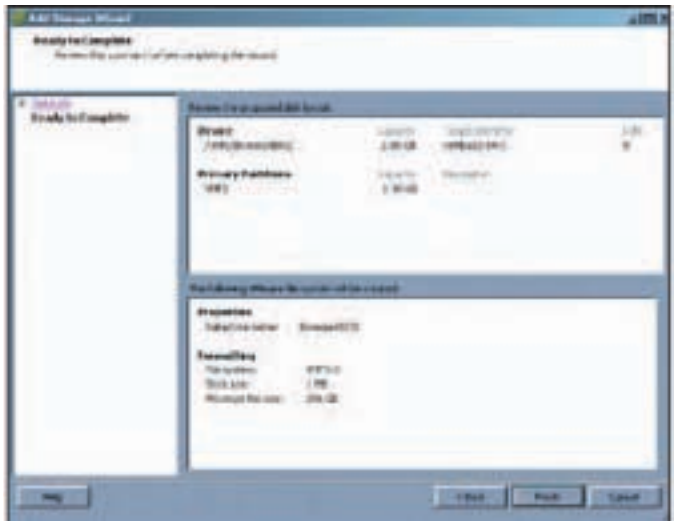


Figure 31 Select the LUN to be used



12. Review the current disk layout on the disk and proceed.

Figure 32 Review disk layout



13. Name the VMFS datastore to be created. Again, give it a meaningful name so it can be easily identified.

Figure 33 Name the VMFS Datastore

14. Specify the maximum file size allowed on the datastore and the maximum capacity on the datastore.

Figure 34 Specify file size and capacity

15. Review the summary and proceed to create the VMFS datastore.

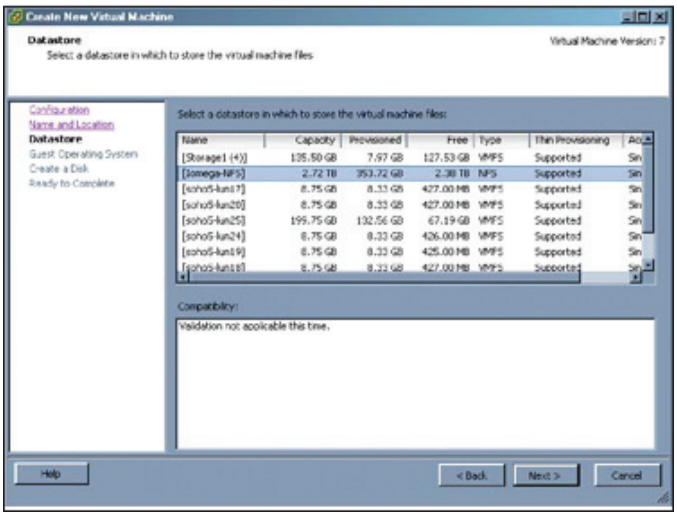
Figure 35 Create VMFS datastore

ADDING AN RDM DISK TO VIRTUAL MACHINE

A raw device mapping (RDM) is a special file in a VMFS volume that acts as a proxy for a raw device. The RDM provides some of the advantages of a virtual disk in the VMFS file system, while keeping some advantages of direct access to raw devices. VMware recommends RDM when a virtual machine must interact with a real disk on the SAN or iSCSI SAN. Two compatibility modes are available for RDM. The physical compatibility mode (a.k.a. pass-through mode) allows direct access of a SCSI device for those applications that need lower-level control. The virtual

compatibility mode (a.k.a. non pass-through mode) allows an RDM to act exactly like a virtual disk file.

Prior to adding RDM, we need to create a virtual machine first. An iSCSI LUN on the StorCenter NAS can then be

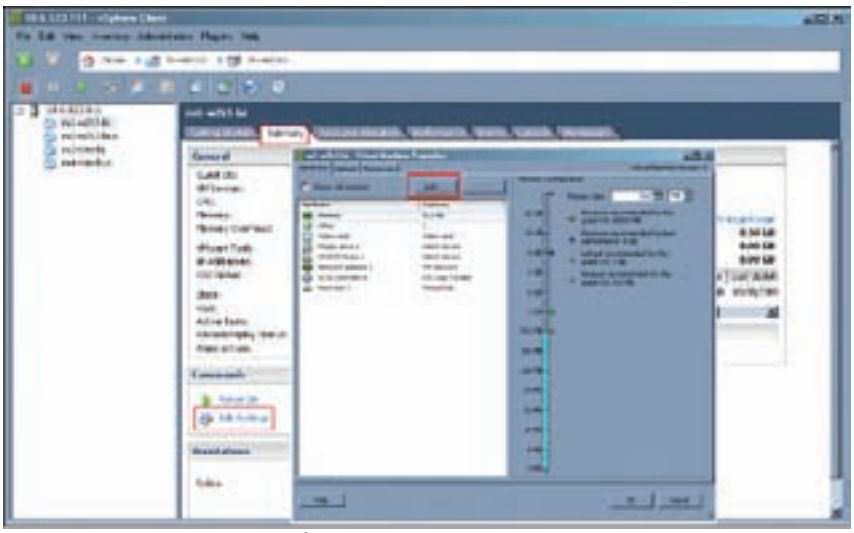


assigned to the virtual machine in either compatibility mode.

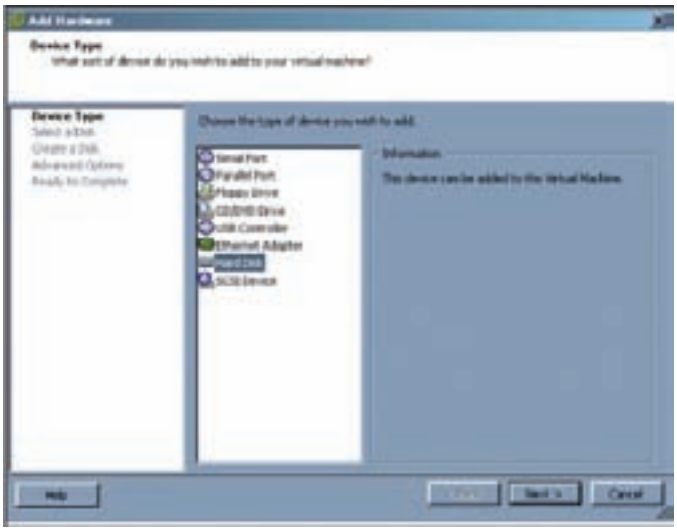
1. Go to **Inventory › Host › New Virtual Machine...** to create a new virtual machine. After naming the virtual machine, select a datastore in which to store the files for the virtual machine. For illustration purposes, the "Iomega-NFS" datastore created previously is used in the following figure.

Figure 36 Choose the datastore to hold the virtual machine

2. Follow the instructions on setting the Guest Operating System, CPUs, Memory, Network, and Virtual Disk Capacity to complete the process of virtual machine creation.

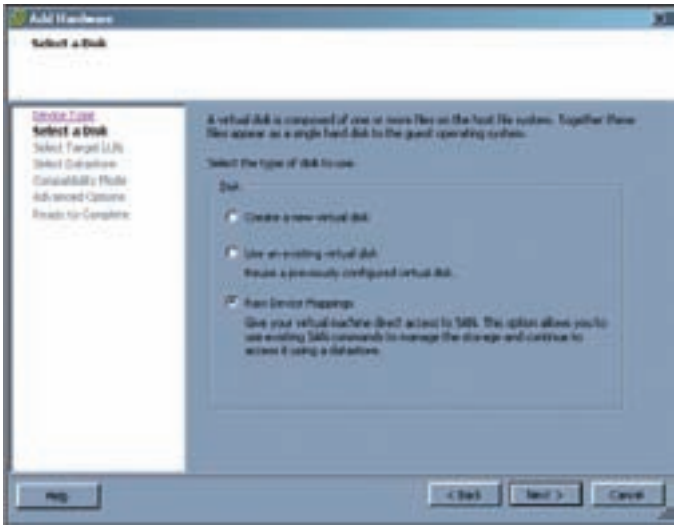


3. Install the guest Operating System using a CD/DVD or ISO image. Power on the virtual machine after installation to finish all virtual machine configurations.



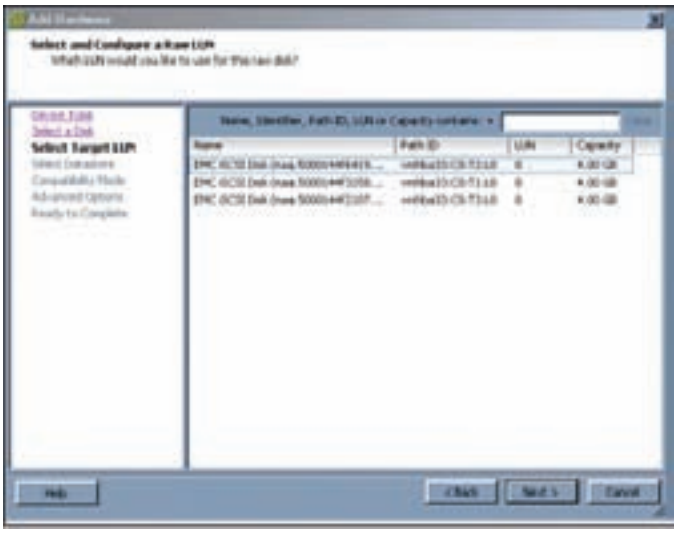
4. Go to **Summary › Edit Settings** with the virtual machine powered on or powered off. When in the Virtual Machine Properties window, click Add to add a new hardware to the virtual machine.

Figure 37 Edit virtual machine settings



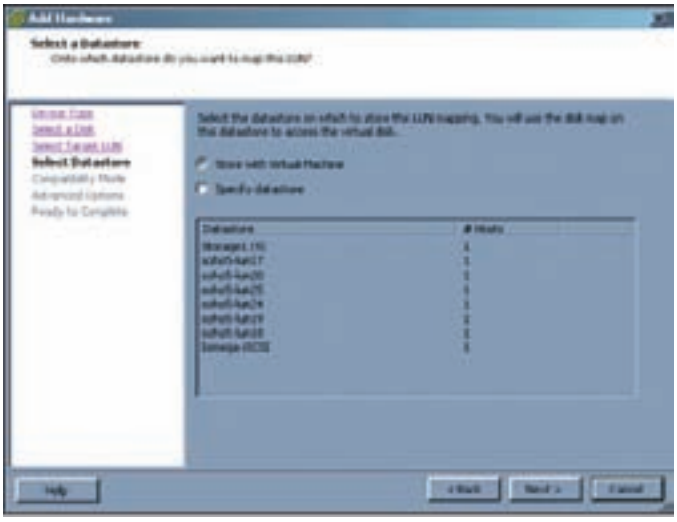
5. Select Hard Disk as the hardware to add.

Figure 38 Add a hard disk to virtual machine



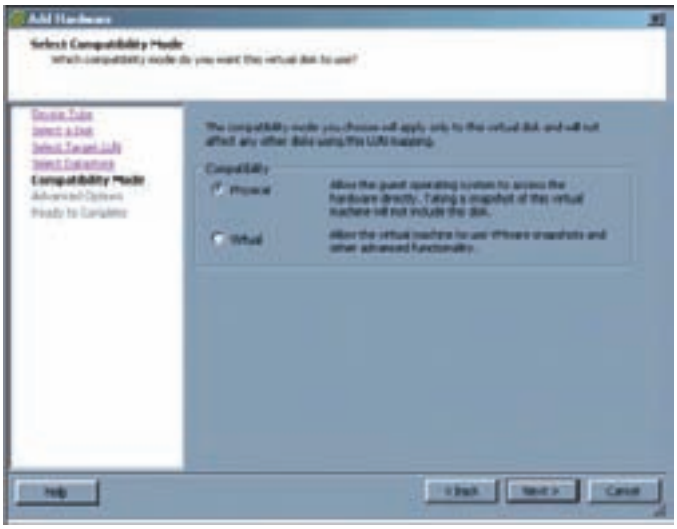
6. Choose Raw Device Mappings as the virtual disk type.

Figure 39 Select RDM as the disk type



7. Select the iSCSI LUN on the StorCenter NAS to be used as an RDM disk.

Figure 40 Select the LUN to be used as the RDM



8. Choose which datastore to map to the RDM. The default is to store the RDM with the virtual machine in the same datastore.

Figure 41 Decide where to map the RDM

9. Select which RDM compatibility mode to use.

Figure 42 Select the compatibility mode

10. Choose the default virtual device/SCSI node and have the RDM disk added into the virtual machine.

11. After the RDM disk is added from ESX Server, the virtual machine needs to rescan its SCSI bus to discover the new disk. Afterwards, partitions can be created and formatted with a file system type. For a Windows guest, use the Disk Manager utility; for a Linux guest, use the fdisk utility and file system formatting tools such as mkreiserfs.

MULTIPATHING AND FAILOVER CONSIDERATIONS

An important aspect when configuring an ESX Server network is to ensure that there is redundancy to the ESX Server's storage. This redundancy is available when the storage is being accessed by either the NFS protocol or the iSCSI protocol.

Most of the Iomega StorCenter NAS server has at least two Gigabit Ethernet ports. The px6-300d we used in this document has dual Gigabit Ethernet ports on the device, so redundant network can be configured to allow multiple paths into storage. Highly available network can also be configured on the ESX Server side to prevent access to storage being lost in case of a NIC or switch failure. The mechanism on the ESX Server is to configure NIC Teaming between two or more NICs connected to the same subnet. Additionally, two Ethernet switches configured with the

same subnet and connected by an uplink can be configured.

To configure NIC teaming on the StorCenter px6-300d storage device:

1. Go to **Network › Network.**

Figure 43 Configure StorCenter px6-300d network settings

2. Click on “Modify network settings”. Select “Failover” as “Bonding Mode” and click Apply. Click Yes at the warning message appearing.

Figure 44 Network Settings on StorCenter px6-300d

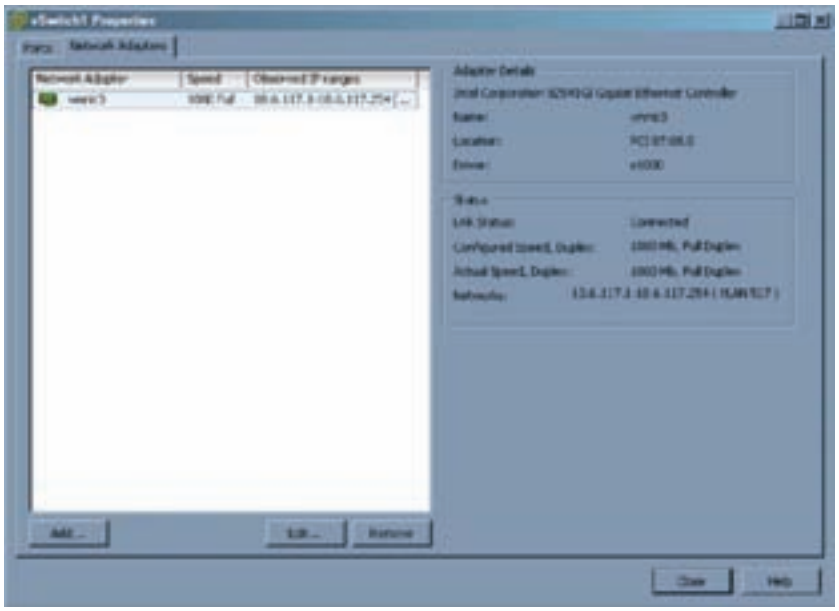
3. Click on the first network interface to open the associated tab. Click on “Bond Network Interface”.

Figure 45 Bond interface on StorCenter px6-300d

4. Select Nic 2 and click Apply. Network configuration changes require the StorCenter px6-300d device software to be restarted. You have to confirm this on the following windows appearing.

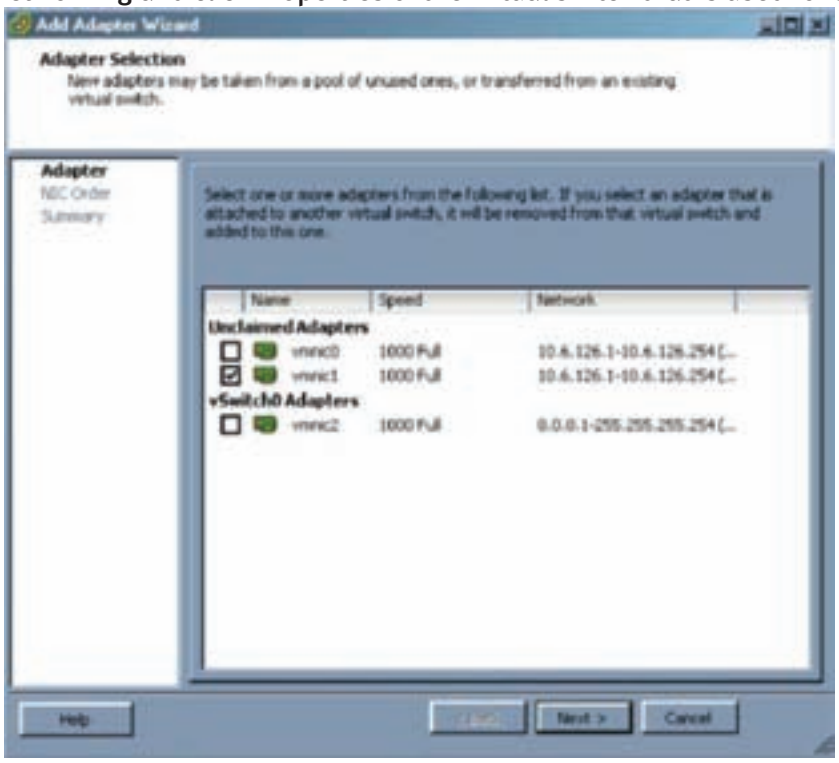
After the restart has been completed, the Network page looks like this:

Figure 46 Bonded network interfaces



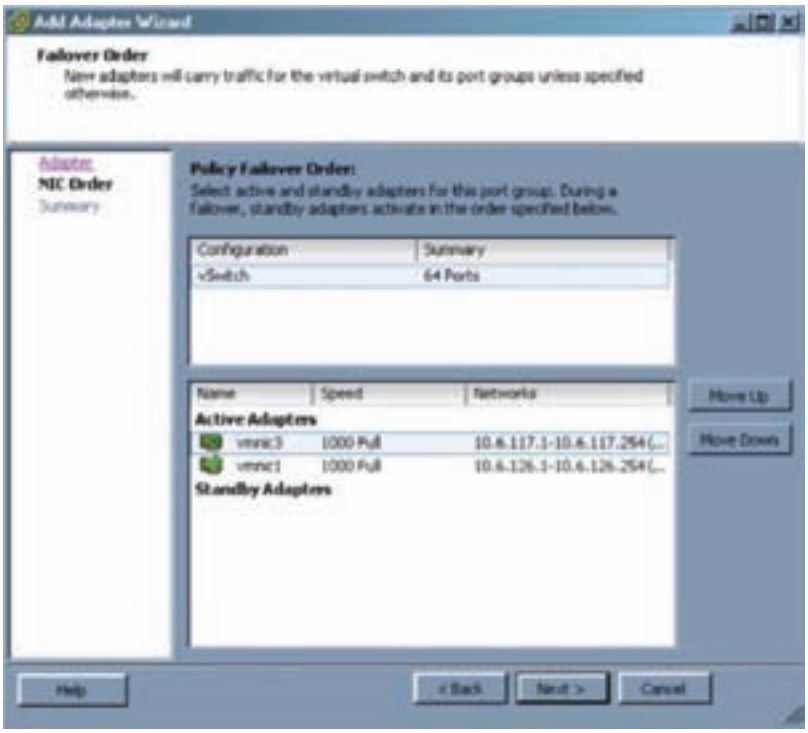
To configure NIC teaming on the ESX server:

1. Go to **Configuration › Networking** and click **Properties** of the virtual switch that is used for storage connectivity.



2. Click the Network Adapters tab and then the **Add** button.

Figure 47 Add a network adapter to virtual switch



3. Select one of the unclaimed network adapters to add to the virtual switch.

Figure 48 Select the network adapter to add

4. Decide which adapter(s) are active and standby.

Figure 49 Set active and standby adapter(s)

5. After the network adapter is added, the virtual switch should show two adapters.

Figure 50 Virtual switch with NIC teaming

NIC teaming is the solution for providing highly available NFS storage connection from the ESX server to the StorCenter NAS device. However, to provide high availability for iSCSI storage connection, a different solution should be used.

The VMware ESX software iSCSI initiator was completely rewritten for vSphere 4. One of the biggest improvements of the initiator is the native multipathing support that allows more than one physical path to transfer data between

the ESX host and the storage device. In case of a failure of any element in the iSCSI network, ESX can switch to another physical path. Additionally, multipathing provides load balancing across multiple physical paths to reduce or remove potential bottlenecks. By default, ESX provides an extensible multipathing module called the Native Multipathing Plugin (NMP) to manage the function.

Important: With vSphere iSCSI multipathing, the VMKernel routing table is bypassed. Therefore, VMware officially requires that the iSCSI initiator and the iSCSI target are placed on the same subnet to avoid routing. Otherwise, the ESX 4.0 iSCSI initiator cannot connect to the iSCSI target. See VMware Knowledge Base article KB1009524 for details. The follow procedure assumes that the initiator and target are on the same subnet.

By default, iSCSI multipathing is not enabled in vSphere 4. To use the feature, you must have two or more NICs to designate for iSCSI and they need to be connected to a single vSwitch. Each VMKernel port is associated with one network adapter using 1:1 mapping.

To configure multipathing in ESX Server 4:

1. Follow the steps described above in NIC teaming configuration to add a network adapter.
2. Create a new VMkernel port for the new network adapter, the number of VMkernel ports must correspond to the number of network adapters on the vSwitch. Follow the steps described in the VMkernel port configuration section.

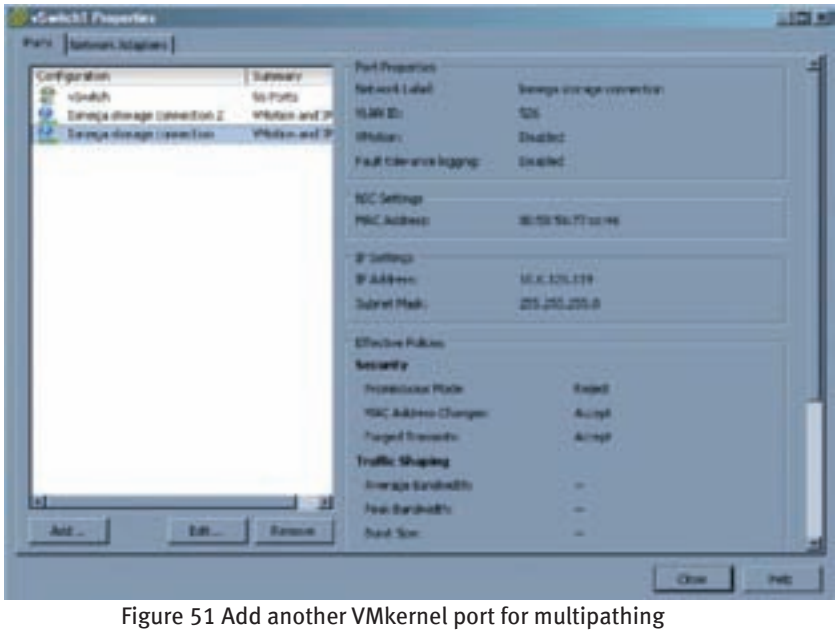


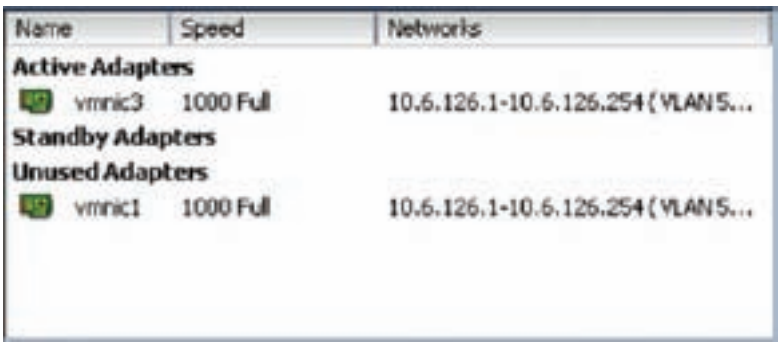
Figure 51 Add another VMkernel port for multipathing

3. By default for each VMkernel port on the vSwitch, all network adapters are active. This setup must be modified so that each port maps to only one corresponding active adapter.
   a. Go to Properties of the vSwitch, select the VMkernel port to modify and click Edit.

Figure 52 Edit VMkernel port

   b. In the NIC Teaming tab check Override vSwitch failover order.

   c. Designate one NIC as the active adapter, and click the Move Down button to make the other NIC as an



unused adapter.

Figure 53 Override vSwitch failover order for one VMkernel port

d. Repeat the steps to modify the other VMkernel port. In this example, VMkernel port Iomega storage connection is associated with vmnic1 and VMkernel port Iomega storage connection 2 is associated with vmnic3. Go to Properties of the vSwitch, select the VMkernel port to modify and click Edit.

Figure 54 Override vSwitch failover order for another VMkernel port

4. Find the ESX iSCSI software initiator as shown in Figure 29.

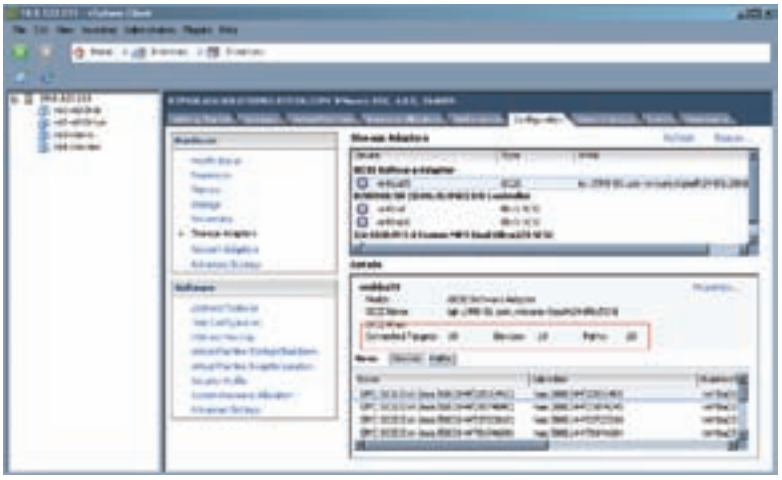
5. Using the vSphere CLI, connect the software iSCSI initiator to the iSCSI VMkernel ports.

```
# esxcli swiscsi nic add –n vmk0 –d vmhba33
# esxcli swiscsi nic add –n vmk1 –d vmhba33
```

6. Verify the iSCSI initiator configuration with both VMkernel ports listed.

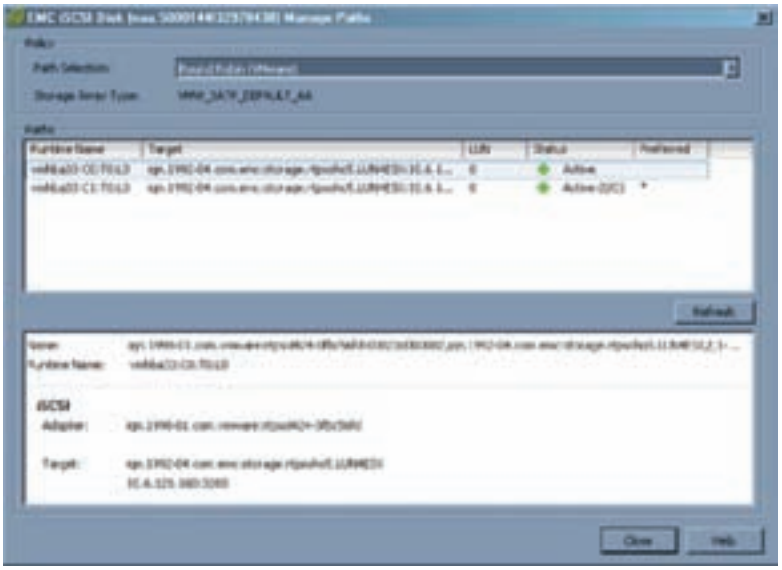
```
# esxcli swiscsi nic list –d vmhba33
vmk0
    pNic name: vmnic1
    ipv4 address: 10.6.126.119 ipv4 net mask: 255.255.255.0 ipv6 addresses:
    mac address: 00:04:23:d7:5f:45 mtu: 1500
    toe: false tso: true
    tcp checksum: false vlan: true
    link connected: true ethernet speed: 1000 packets received: 3227008 packets sent: 694822
    NIC driver: e1000
    driver version: 8.0.3.1-NAPI
    firmware version: N/A

vmk1
    pNic name: vmnic3
    ipv4 address: 10.6.126.120 ipv4 net mask: 255.255.255.0 ipv6 addresses:
    mac address: 00:11:43:e7:e4:12 mtu: 1500
    toe: false tso: true
    tcp checksum: false vlan: true
    link connected: true ethernet speed: 1000 packets received: 2472636 packets sent: 172361
    NIC driver: e1000
```



```
    driver version: 8.0.3.1-NAPI
```

firmware version: N/A

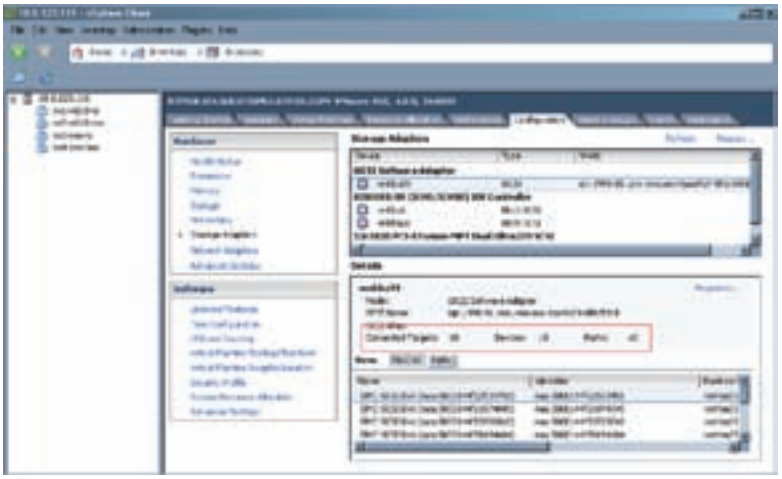


7. Rescan the iSCSI host bus adapter to add the extra paths from the initiator to the target. The total number of paths should be doubled due to the additional network adapter being bound to the initiator.

Figure 55 Double the number of iSCSI paths

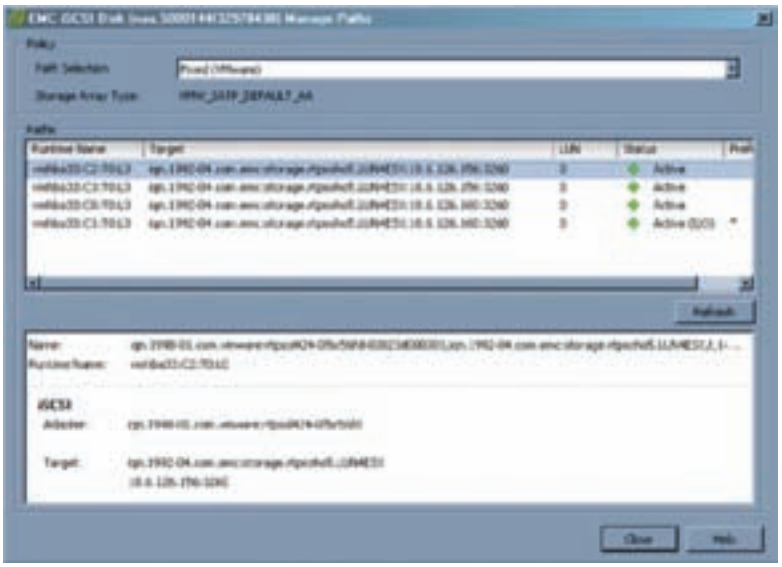
8. Right-click on the iSCSI device and select Manage Paths to set path selection policy.

Figure 56 Set path selection policy



9. When using multipathing, NIC teaming is not recommended on the StorCenter NAS device. Follow Figure 26 to add the other iSCSI target of the StorCenter NAS device and rescan the iSCSI host bus adapter.

10. Since both of the iSCSI targets contain the same set of LUNs, the total number of connected targets and devices



on ESX server remain the same. However, the total number of paths is again doubled.

Figure 57 Double the number of paths with additional target

11. Each device now has four paths in a full-mesh topology between the two NICs on the ESX server and the two on the storage device.

Figure 58 Full-mesh path topology

12. The number of paths can also be confirmed on the StorCenter NAS device.
Go to **Storage › iSCSI** and click on the iSCSI LUN to open the associated tab. Click on “Connected Clients”.

Figure 59 Confirm paths on Iomega NAS device

CONCLUSION

VMware vSphere dramatically improves the efficiency and availability of resources and applications in organizations of any sizes. VMware customers typically save 50-70% on overall IT costs by lowering both capital and operational costs and improving operational efficiency and flexibility. This is especially important to small businesses that normally have a very limited IT budget.

The Iomega StorCenter NAS Servers are high-performance, ease-of-use, and highly reliable storage devices, specifically designed to meet the storage challenges that small- and medium businesses facing daily. The NAS servers are supporting the NFS- and iSCSI protocol, the two predominant ways of utilizing IP storage by the VMware ESX Server. Customers' total infrastructure costs are further reduced by using an existing Ethernet infrastructure.

The Iomega StorCenter NAS Servers are certified in the VMware Hardware Compatibility List as both NAS and Software iSCSI storage. It provides reliable and proven storage solutions to small- and medium businesses that plan to deploy VMware vSphere.