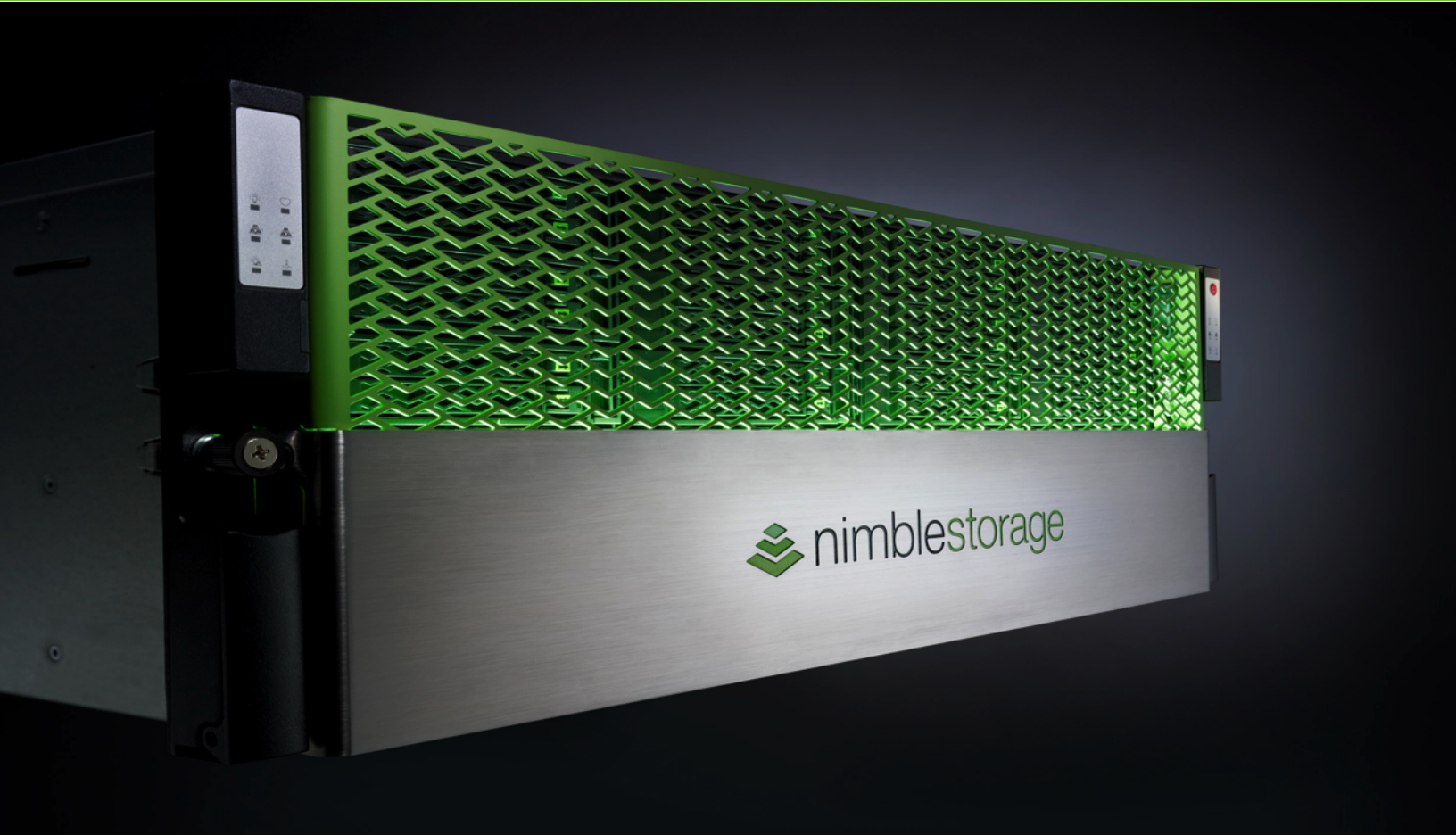




a Hewlett Packard Enterprise company



VMware Integration Guide

Version 4.x

Legal Notices

Copyright 2010-2017 Hewlett Packard Enterprise Development LP. All rights reserved worldwide.

No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by electronic, mechanical, recording, photocopy, scanning or other means without prior written permission from Nimble Storage, Inc.

The product described in this documentation may be protected by US Patent 8,285,918, US Patent 8,832,330 US Patent 8,924,607, US Patent 8,949,502, US Patent 9,003,113, US Patent 9,015,406, US Patent 9,081,670, US Patent 9,098,405, US Patent 9,116,630 and other pending patent applications.

Nimble Storage, Incorporated (Nimble), has used the latest information that is available in producing this document. Nimble Storage makes no warranty, expressed or implied, with regard to accuracy and completeness.

Information in this document is subject to change without notice.

Nimble Storage Inc. Nimble Storage, the "Nimble Storage" logo, InfoSight, SmartStack, CASL, NimbleConnect, Timeless Storage, Data Velocity Delivered, Unified Flash Fabric, and other names are registered trademarks or trademarks of Nimble Storage in the United States and/or other jurisdictions. Other trade names, trademarks, and service marks are the property of their respective owners.

InfoSight® is a registered trademark in Japan of Intage Inc. of Japan. Usage of InfoSight® in Japan is permitted pursuant to a trademark license agreement between Nimble Storage, Inc. and Intage Inc.

Nimble Storage, Inc.
211 River Oaks Parkway
San Jose, CA 95134
U.S.A.

Tel: +1 408.432.9600
Website: <http://www.nimblestorage.com>
Sales: sales@nimblestorage.com

Publication Date: Thursday July 13, 2017 14:58:21

Support

All documentation and knowledge base articles are available on the Nimble Storage Support site at <https://www.nimblestorage.com>. To register on InfoSight, click the *Enroll Now* link on the main page.

Email: support@nimblestorage.com

For all other general support contact information, go to <https://www.nimblestorage.com/customer-support/>.

Contents

Nimble VMware Integration.....	7
VMware Integration Features.....	7
VIBs.....	8
Before You Integrate.....	8
Manual VMware iSCSI configuration.....	9
Overview.....	9
Configure ESXi iSCSI Networking with Multiple vSwitches	9
Configure ESXi iSCSI Networking with a Single vSwitch.....	15
Configure the ESXi iSCSI Software Adapter	27
Bind VMK Ports to ESXi iSCSI Software Adapter (ESXi 5.0, 5.1, 5.5, 6.0, and 6.5).....	29
Nimble Connection Manager.....	33
Understand the Nimble Connection Manager.....	33
NCM Installation.....	36
Copy NCM to the ESXi Host.....	37
Install NCM When vCenter Has Internet Connection.....	38
Install NCM When vCenter Has No Internet Connection.....	39
Download the NCM Installation Package.....	40
Install NCM Online Bundle Through ESXCLI.....	41
Install NCM Offline Bundle Through ESXCLI.....	42
Verify NCM Installation.....	43
Configure NCM on the ESXi Host.....	43
View NCM Logs.....	44
Update NCM.....	44
Uninstall NCM.....	45
VMware Synchronized Snapshots.....	46
How Nimble Synchronization Works with VMware.....	46
Snapshot Exclusion and Inclusion Options for VMs and Datastores	47
Volume Collections and VMware Objects.....	49
Common Tasks and Best Practices.....	50
VMware Partition Alignment.....	50
Register or Add VM to Inventory.....	50
ESXi Host.....	51

vCenter Server.....	51
Restore Entire Datastore to an Earlier Snapshot.....	51
Recover a VMware Volume from a Cloned Snapshot	52
Change the VMware vCenter Access Information.....	53
Change Access Information Using the Editing Wizard.....	53
Change Access Information Using the CLI.....	53
VMware iSCSI Best Practices.....	53
VM Guest Machines.....	54
Managing Target Subnets.....	56
Rapid Cloning of a VM Using Nimble's LUN Cloning.....	57
Prepare a VM or a LUN as a Template.....	57
Perform Steps on the Guest OS.....	57
Create a VM Clone.....	58
Using VMware RDM disks	59
Nimble LUNs in the Device List.....	59
Locate vCenter logs.....	59
Unresponsive vCenter.....	60
VAAI Integration.....	61
What is VAAI?.....	61
Enable the VMware VAAI Provider to use Nimble Volumes.....	61
The Nimble vCenter Plugin.....	63
Register the vCenter Plugin Using the NimbleOS CLI.....	63
Register the vCenter Plugin Using the NimbleOS GUI.....	64
View a List of Registered Plugins.....	64
Create Roles (Role-Based Permissions).....	65
Create a New Datastore.....	67
Clone a Datastore.....	71
Grow a Datastore.....	72
View Datastore Details.....	73
Take a Snapshot of a Nimble-based Datastore.....	74
Delete a Nimble-based Datastore.....	75
Unregister the vCenter Plugin Using NimbleOS CLI.....	75
Unregister the vCenter Plugin Using NimbleOS GUI.....	76
Unregister the vCenter Plugin Using the vCenter Server.....	76
The Nimble vCenter Web Client Plugin.....	78
Register the vCenter Web Client Plugin.....	78
Create Roles (Role-Based Privileges).....	78
Create a New Datastore.....	81
Mount an Existing Datastore.....	85
Clone a Datastore.....	86

Grow a Datastore.....	87
View Datastore Details.....	87
Take a Snapshot of a Nimble-based Datastore.....	89
Edit a Nimble-based Datastore.....	90
Enable iSCSI Digest.....	93
Disable iSCSI Digest.....	94
Delete a Nimble-based Datastore.....	94
Unregister vCenter Web Plugin.....	94
Virtual Volumes (VVols).....	95
How VASA Provider Works with VVols.....	95
Protocol Endpoints.....	95
VVols and Nimble Connection Manager.....	96
Supported Features.....	96
Encryption.....	96
NWT.....	96
Storage Policy Based Management (SPBM).....	96
Group and Pool Merges.....	97
Configuring VVols.....	97
VVols Workflow.....	97
Add a vCenter Server.....	97
Register a vCenter Server Extension.....	98
Create a VVol Datastore.....	98
Create a VM.....	98
Managing VVols.....	99
Role-Based Access Control (RBAC).....	100
Using VASA Provider to provide disaster recovery for VVols.....	100
Troubleshooting Tips.....	101
Registration Error - Invalid Provider Certificate.....	101
Failure to Add VP - Time Mismatch.....	101
Datastore Inaccessible.....	102
Nimble SRM Integration.....	103
How SRA works with SRM.....	103
Overview of SRA Setup Process.....	103
SRA for SRM Prerequisites.....	105
Download the SRA for SRM Installation Package.....	105
Install SRA for SRM.....	106
Update SRA for SRM.....	107
Un-install SRA for SRM.....	109
Configuring SRM and SRA to work with Nimble storage arrays.....	109
Initiate a Recovery Plan.....	110
Test the Recovery Plan.....	111

Implement the Recovery Plan.....	111
Usage of Nimble SRA with Microsoft Volume Shadow Service (VSS)	112

Helpful Information.....113

Configure iSCSI Discovery.....	113
iSCSI Host Connection Methods.....	119
Set the iSCSI Host Connection Method to Manual.....	124
Configure Jumbo Frames.....	124
Change NIC Frame Size.....	127
Change NIC Frame Size.....	127
Configure an ESX Datastore.....	127
Set the Path Selection Policy to Round Robin (ESXi 5.0, 5.1, 5.5, and 6.0).....	131
Enable Application-Consistent Quiescing on Windows Server 2008 VM.....	132
Log in to the NimbleOS CLI.....	133
Set up a Serial Connection.....	134
Set up a Direct Connection.....	135
iSCSI Initiator Groups.....	136
Create an iSCSI Initiator Group Using the GUI.....	137
Create an iSCSI Initiator Group.....	138
Assign Volumes to an iSCSI Initiator Group Using the GUI.....	139
Assign Volumes to an iSCSI Initiator Group Using the CLI.....	139
Unassign Volumes from an iSCSI Initiator Group Using the GUI.....	140
Unassign Volumes from an iSCSI Initiator Group Using the CLI.....	140
Edit an iSCSI Initiator Group Using the GUI.....	140
Edit an iSCSI Initiator Group Using the CLI.....	141
Delete an iSCSI Initiator Group Using the GUI.....	142
Delete an iSCSI Initiator Group Using the CLI.....	143

Nimble VMware Integration

Nimble Storage gives you multiple ways to access and integrate with the VMware environment.

Important For best results, please review the VMware integration [Requirements](#) on page 8.

VMware Integration Features

Most integration features are part of the NimbleOS that ships pre-installed on the Nimble array. However, certain features require you to install them.

- The Nimble vCenter plugin is a component of the NimbleOS that runs on the Nimble array. The plugin comes pre-installed, but you must register it with vCenter so it can manage VMware datastores on the array. See [The Nimble vCenter Plugin](#) on page 63.
- Nimble Storage Replication Adapter (SRA) is an optional component that installs on the Windows server that runs the VMware Site Recovery Manager (SRM). SRA lets you set up disaster recovery plans. See [Nimble SRM Integration](#) on page 103.
- Nimble Connection Manager (NCM) is an optional package that installs on the ESXi 5.0, 5.1, 5.5, or 6.0 host. NCM automatically creates the optimal number of iSCSI sessions for each Nimble volume and manages the selection of paths to the volumes. See [Nimble Connection Manager](#) on page 33.

VMware integration consists of the following features:

VAAI

Enables WRITE SAME, UNMAP, THIN PROVISION STUN, ATS, and XCOPY APIs.

Located in: NimbleOS

Component: Built-in NimbleOS

VASA Provider

Enables management of Virtual Volumes (VVols) by providing information about VVols and Storage-Based Policy Management (SBPM). VASA 3.0 provides disaster recovery by replicating the VVols assigned to a Replication Group. You must register VASA Provider with vSphere.

Located in: NimbleOS

Components: Built-in NimbleOS

vCenter integration

Enables the Nimble-specific plugin within vCenter for creating and managing datastores on the Nimble array.

Located in: NimbleOS

Components: vCenter desktop client and vCenter web-based client plugins

VMware synchronized snapshots

Enables application consistent snapshots within VMware environments.

Located in: NimbleOS

Component: Built-in NimbleOS

SRM integration

Enables integration and interoperability with VMware Site Recovery Manager.

Located in: Nimble SRA for SRM

Component: Nimble Storage Replication Adapter

iSCSI Connection Management

Creates efficient connection management and path management to the Nimble array in a VMware environment.

Located in: Nimble Connection Manager

Components: Nimble Connection Service (NCS), Nimble Path Selection Plugin (PSP)

VIBs

A vSphere Installation Bundle (VIB) is a collection of files packaged into a single archive to facilitate distribution. Nimble Connection Manager (NCM) contains VIBs for the Nimble Connection Service (NCS) and the Nimble Path Selection Plugin (PSP). NCS and PSP are *VMwareAccepted*, which means NCS and PSP were created by Nimble Storage, an approved VMware partner, and are listed in the *VMware Compatibility Guide*.

Before You Integrate

There are a few things to know before setting up your integrated environment.

Requirements

- You must have administrator-level privileges on the VMware vCenter.
- If you are using an iSCSI adapter, HPE recommends that you enable flow control on vNICs.
- If the array is in a VMware environment, you must have ACLs (initiator group and/or CHAP username or WWPN) on all volumes.
- Nimble arrays support jumbo frames when using the iSCSI protocol if your network switches and other components support them.
- Volume alignment is not relevant on a Nimble volume.
- For the vCenter desktop client plugin, you must be running ESX 4.1 or later.
- For the vCenter web-based plugin, you must use vCenter 5.5 Update 1 or later and NimbleOS 2.3.x.
- All firewall ports blocking communications between the Windows machine that is hosting vCenter and the Nimble array must be opened. Ports include:
 - 443 for management and controller communications
 - 4213/4214 for replication
 - 5391/5392 for web service communications

Note If you want to use SSL communication between ESXi hosts and Nimble Storage arrays when you are using VVol datastores, you must use port 8443. Otherwise, ESXi hosts will not be able to mount VVol datastores.

- To gather VM statistics, you must designate the System.Read privilege.

The Nimble vCenter web client plugin supports any web browser that is supported by vCenter.

The best block size for a VMware LUN

On the datastore itself, VMFS provides the SCSI access layer for virtual machines to efficiently read and write data on the underlying disk. It uses adaptive block sizing for large I/Os, and sub-block allocation for small files and directories. VMFS is certified for a wide range of Fibre Channel and iSCSI storage systems, and it is optimized to support large files while also performing many small concurrent writes.

If the Nimble volumes provisioned are set to 4KB block size, you achieve the highest efficiency of data stored: VMware will grab as many or as few of those blocks per write as it needs to create its virtual / variable blocks for the VMs in the datastore. Using large block sizing (for example, 32KB) when the VMFS is using small block writes will artificially consume additional space within the volume.

When provisioning Nimble volumes direct to VM servers, configure the volume performance to match the applications onboard the VM, since this storage isn't coming from the datastore.

Manual VMware iSCSI configuration

Setting up the configuration to ensure that the Nimble Arrays works well with VMware is important. The following section provides all that you need to manually configure the system properly. This setup information applies to all Nimble-VMware installations.

Using the Nimble Connection Manager and Path Selection Plugin is the preferred method of Nimble VMware integration.

Overview

To configure ESXi iSCSI networking, follow this example procedure and perform the tasks in the following order. Details for each task appear in the following pages.

Procedure

- 1 Perform one of these configuration procedures:
 - [Configure ESXi iSCSI Networking with Multiple vSwitches](#) on page 9
 - [Configure ESXi iSCSI Networking with a Single vSwitch](#) on page 15
- 2 [Configure the ESXi iSCSI Software Adapter](#) on page 27
- 3 [Bind VMK Ports to ESXi iSCSI Software Adapter \(ESXi 5.0, 5.1, 5.5, 6.0, and 6.5\)](#) on page 29

Results

After all the above steps are complete, ESXi iSCSI configuration is finished and the Nimble volumes are ready for use as ESXi datastores.

Configure ESXi iSCSI Networking with Multiple vSwitches

To configure ESXi iSCSI networking with the following characteristics:

- Two vmnic ports
- Two vmk ports
- Two vSwitches, with one vmnic port and one vmk port each

The following requirements apply:

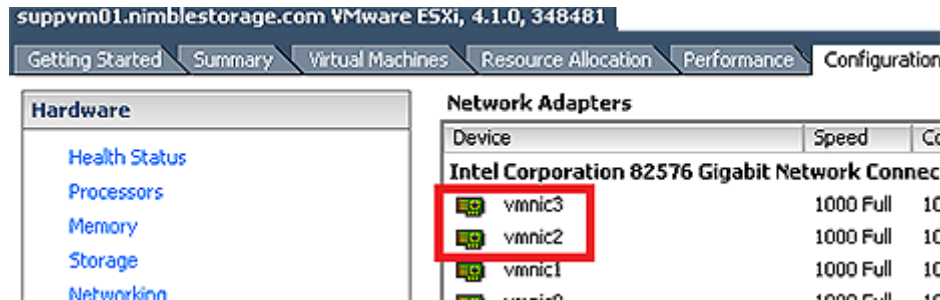
- There must always be a one-to-one relationship between vmnic ports and vmk ports.
For example, if you have four vmnic ports you want to use for iSCSI networking, you must have four vmk ports.
- NIC Teaming must be disabled.
That means each vmk port has only one Active vmnic port, and no Standby vmnic ports.

Using multiple vSwitches with one vmnic port and one vmk port each, enforces the above requirements. NIC Teaming is impossible in this configuration, so it cannot become enabled or configured incorrectly. This is why using multiple vSwitches is the preferred method.

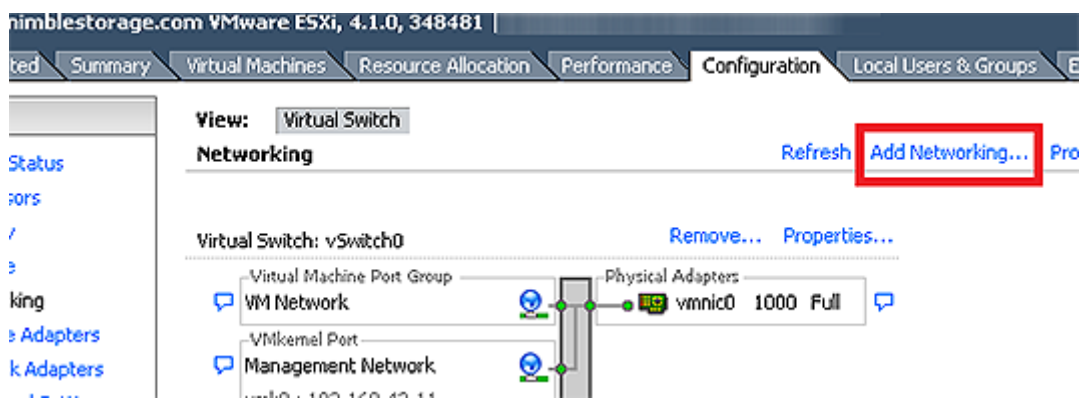
Procedure

- 1 Go to the Configuration / Network Adapters screen on the ESXi host and identify the vmnics you want to use for iSCSI networking.

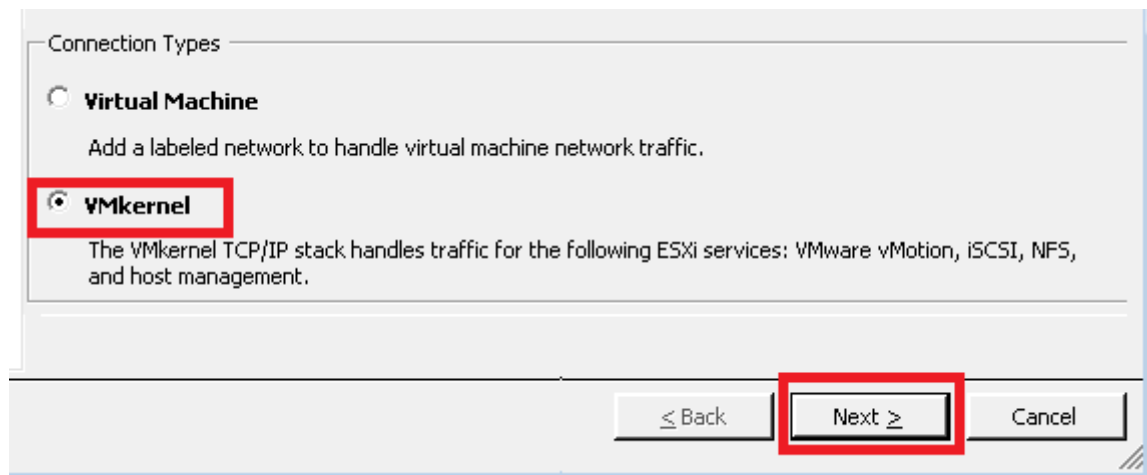
In this example, the ESXi host has a dual-port NIC card, with ports "vmnic2" and "vmnic3."



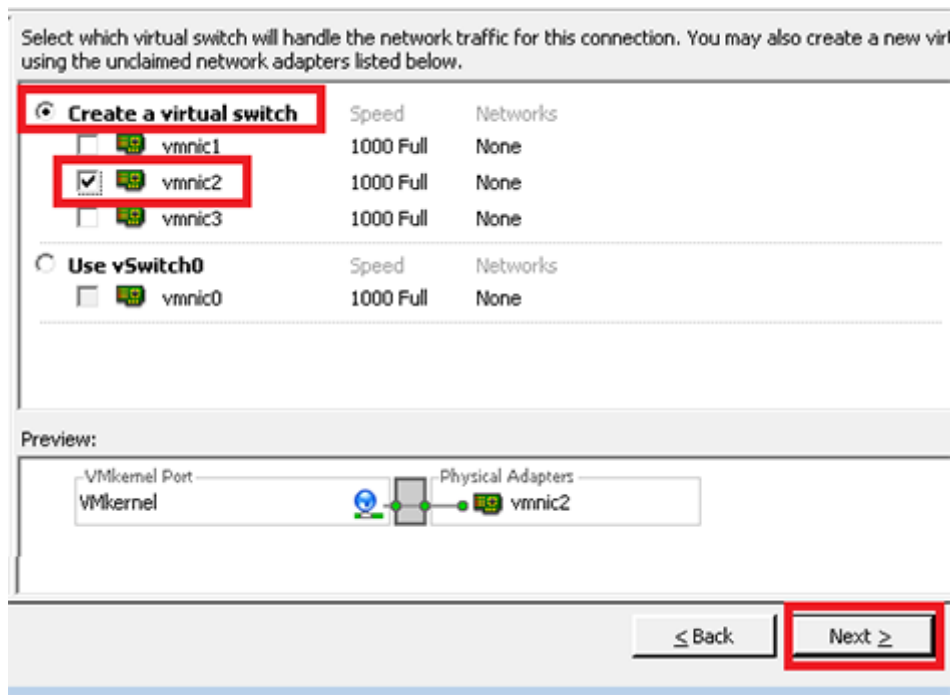
- 2 Go to the Configuration / Networking screen on the ESXi host and click **Add Networking**. In this example, notice that the ESXi host has no iSCSI networking currently configured.



- 3 Select **VMkernel** and click **Next**.

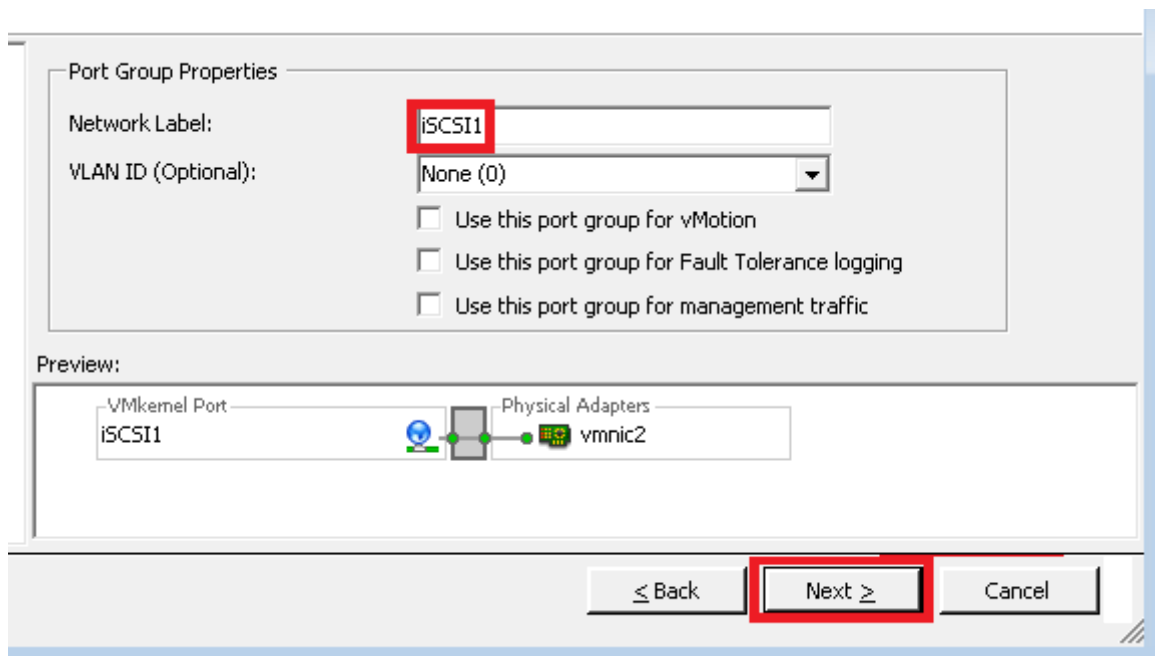


- 4 Select **Create a virtual switch** and the first vmnic port to be used and click **Next**. This example uses *vmnic2*.



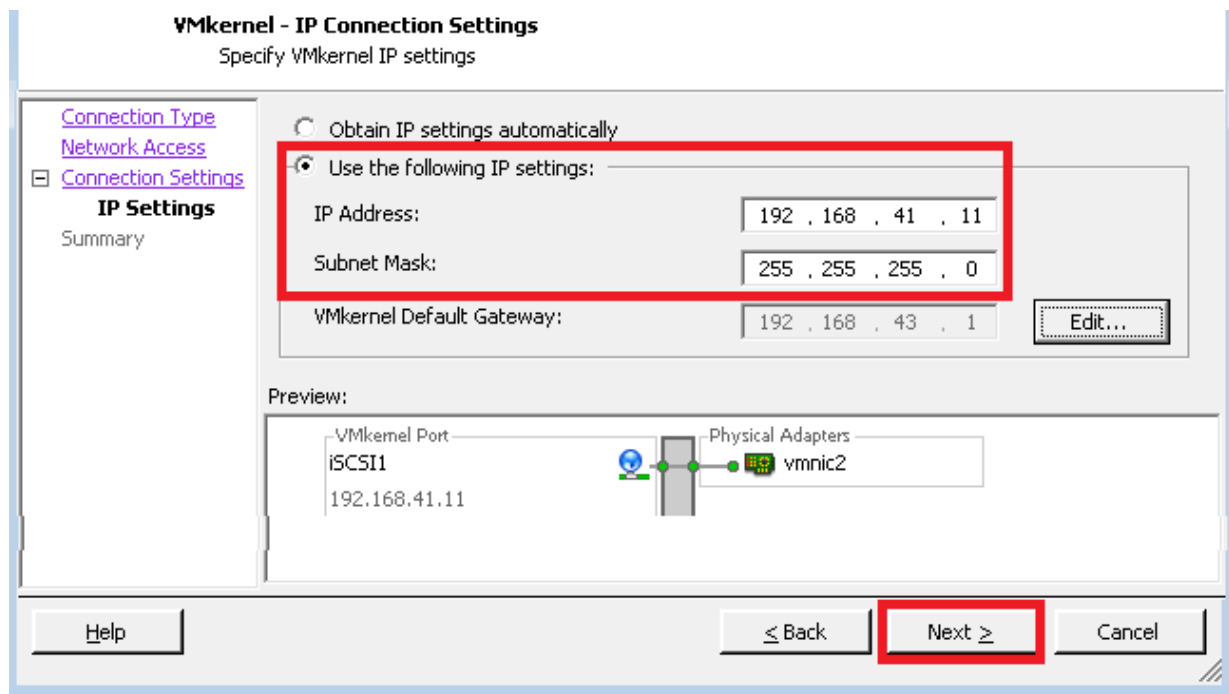
5 Assign a Network Label and click **Next**.

This label must be unique on the ESXi host being configured. This example uses *iSCSI1*.



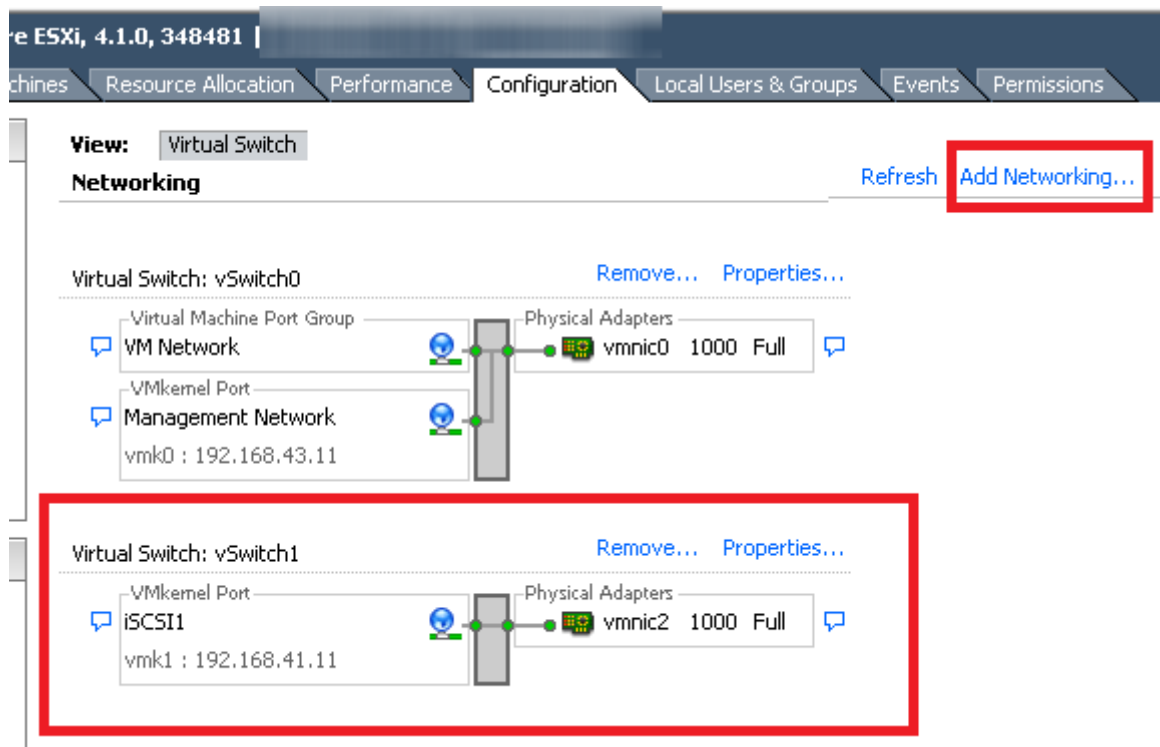
6 Assign an IP address and subnet information for the first vmk port and click **Next**.

This example uses a static IP of 192.168.41.11 and a subnet mask of 255.255.255.0.

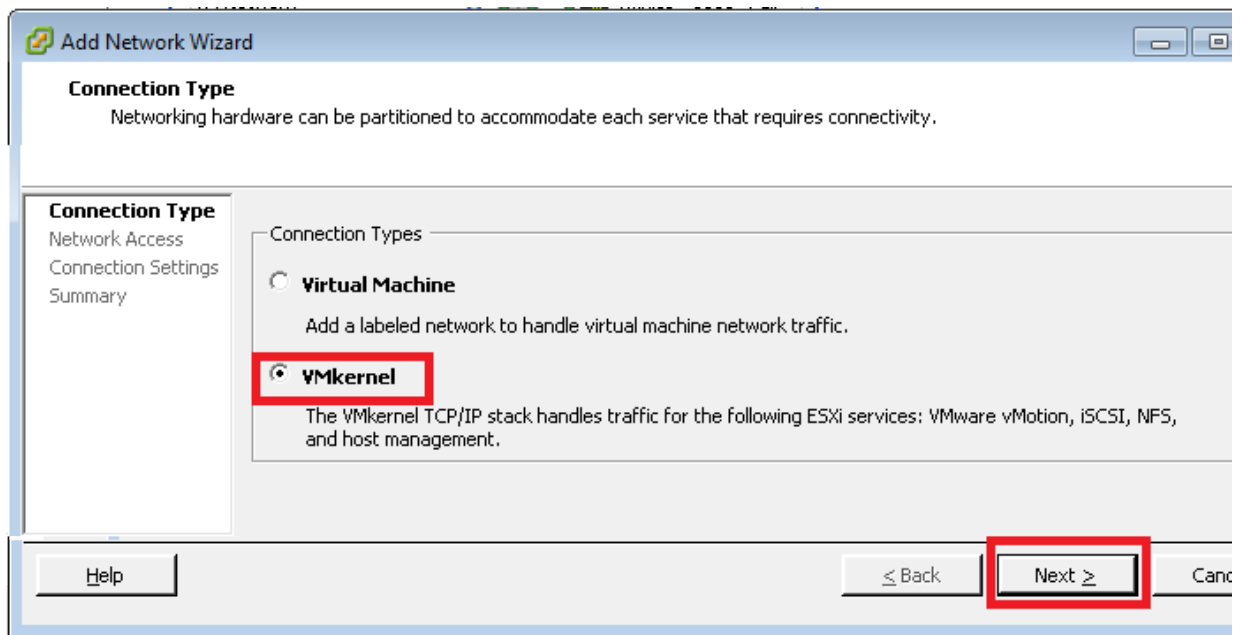


The image shows the 'VMkernel - IP Connection Settings' dialog box. The title bar says 'VMkernel - IP Connection Settings' and the subtitle is 'Specify VMkernel IP settings'. On the left, there is a sidebar with links: 'Connection Type', 'Network Access', 'Connection Settings' (selected), 'IP Settings', and 'Summary'. The main area has two radio buttons: 'Obtain IP settings automatically' (unselected) and 'Use the following IP settings:' (selected). Below the selected option, there are three text boxes: 'IP Address:' with '192 , 168 , 41 , 11', 'Subnet Mask:' with '255 , 255 , 255 , 0', and 'VMkernel Default Gateway:' with '192 , 168 , 43 , 1'. There is an 'Edit...' button next to the gateway. Below this is a 'Preview:' section showing a diagram of a VMkernel Port (iSCSI1, 192.168.41.11) connected to a Physical Adapter (vmnic2). At the bottom, there are buttons: 'Help', '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

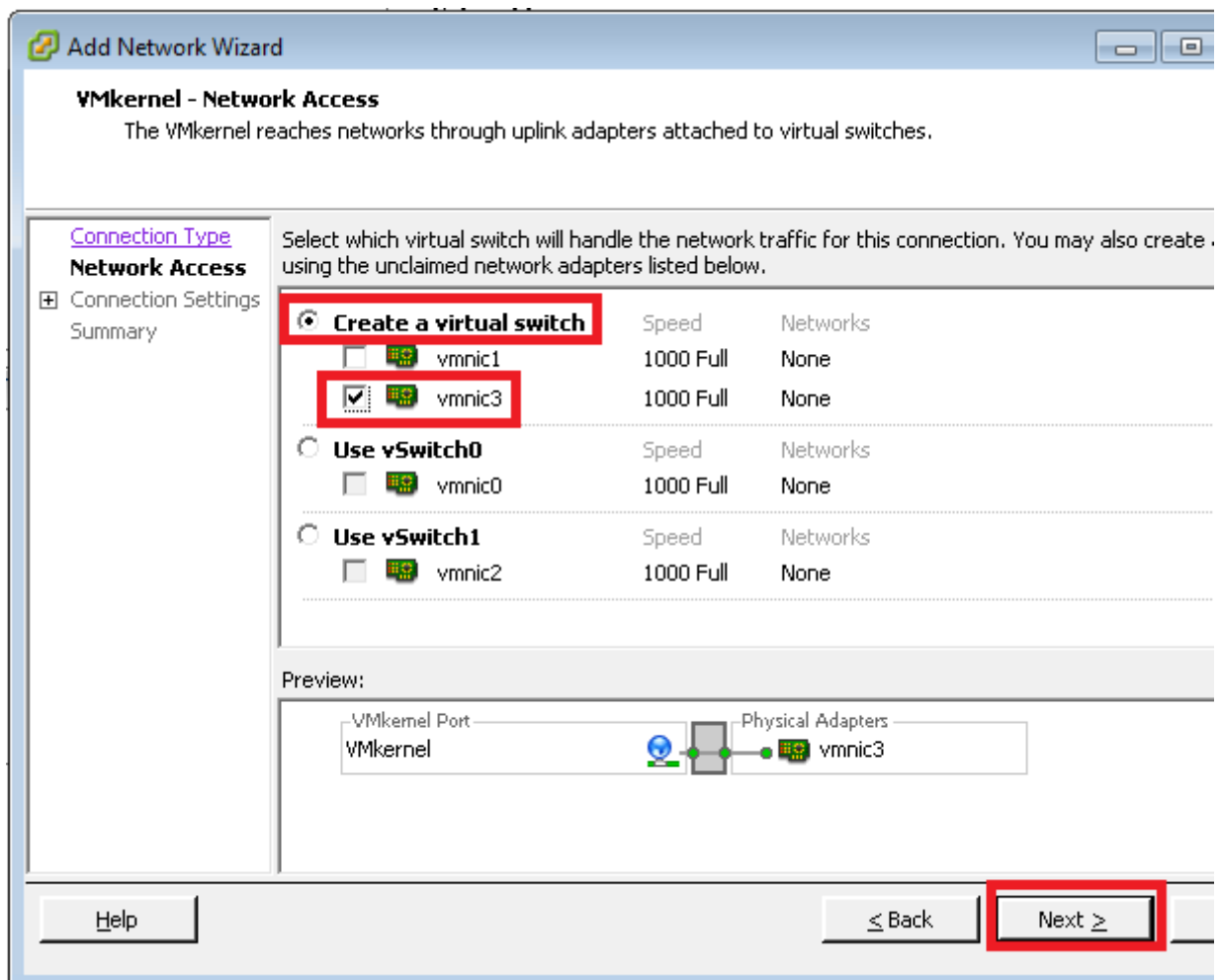
- 7 Review the proposed configuration and if everything is correct, click **Finish**.
The Configuration / Networking screen is updated and displays the new vSwitch and vmk port.
- 8 To start configuring the second switch, click **Add Networking**.



- 9 Select **VMkernel** and click **Next**.



- 10 Select **Create a virtual switch** and the second vmnic port to be used and click **Next**.
This example uses *vmnic3*.



11 Assign a Network Label and click **Next.**

This label must be unique on the ESXi host being configured. This example uses *iSCSI2*.

on Settings
: to identify VMkernel connections while managing your hosts and datacenters.

Port Group Properties

Network Label: **iSCSI2**

VLAN ID (Optional): None (0)

☐ Use this port group for vMotion

☐ Use this port group for Fault Tolerance logging

☐ Use this port group for management traffic

Preview:

VMkernel Port: iSCSI2

Physical Adapters: vmnic3

< Back **Next >**

12 Assign an IP address and subnet information, then click **Next.**

This example uses a static IP of 192.168.41.111 and a subnet mask of 255.255.255.0.

- 13 Review the proposed configuration and if everything is correct, click **Finish**.
The Configuration / Networking screen is updated and displays the new vSwitch and vmk port.

What to do next

Next, go to [Configure the ESXi iSCSI Software Adapter](#) on page 27.

Configure ESXi iSCSI Networking with a Single vSwitch

To configure ESXi iSCSI networking with the following characteristics:

- Two vmnic ports
- Two vmk ports
- One vSwitch, containing both vmnic ports, and both vmk ports
- NIC Teaming disabled

The following requirements apply:

- There must always be a one-to-one relationship between vmnic ports and vmk ports.

For example, if you have four vmnic ports you want to use for iSCSI networking, you must have four vmk ports.

- NIC Teaming must be disabled.

That means each vmk port has only one Active vmnic port, and no Standby vmnic ports.

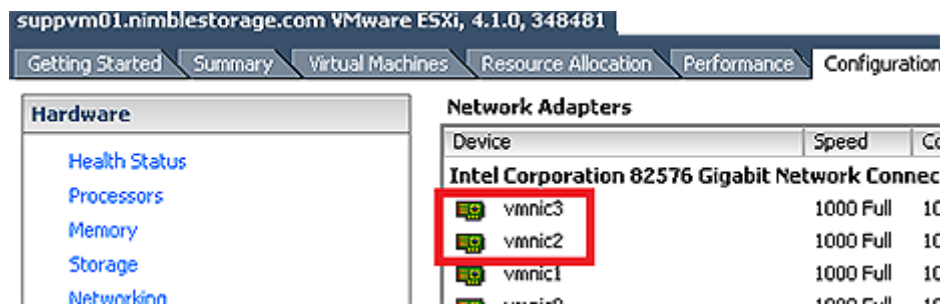
When a vSwitch used for iSCSI has more than one vmnic, NIC Teaming must be disabled. Follow the steps in this procedure to disable NIC Teaming.

Before you begin

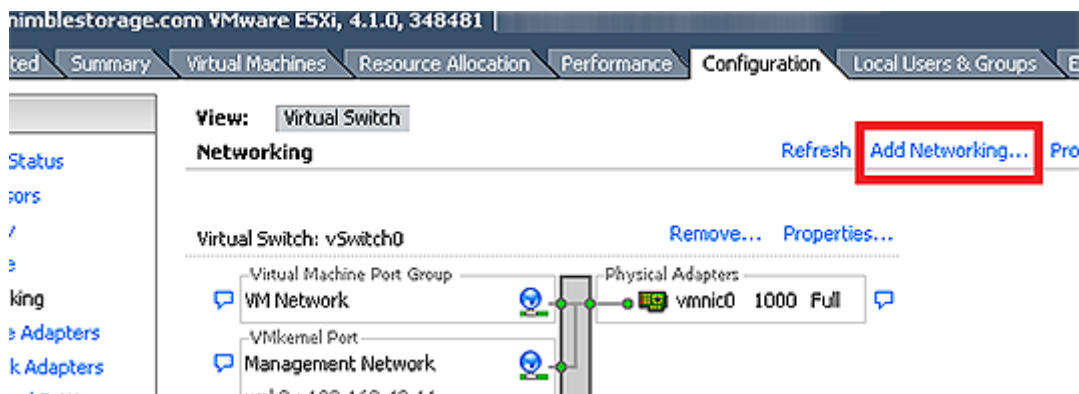
Procedure

- 1 Go to the Configuration / Network Adapters screen on the ESXi host and identify the vmnics you want to use for iSCSI networking.

In this example, the ESXi host has a dual-port NIC card, with ports "vmnic2" and "vmnic3."



- 2 Go to the Configuration / Networking screen on the ESXi host and click **Add Networking**. In this example, notice that the ESXi host has no iSCSI networking currently configured.



- 3 Select **VMkernel** and click **Next**.

Connection Types

☐ **Virtual Machine**
Add a labeled network to handle virtual machine network traffic.

☒ **VMkernel**
The VMkernel TCP/IP stack handles traffic for the following ESXi services: VMware vMotion, iSCSI, NFS, and host management.

≤ Back **Next >** Cancel

- 4 Choose **Create a virtual switch** and the two vmnic ports to be used, then click **Next**.
This example uses "vmnic2" and "vmnic3."

Select which virtual switch will handle the network traffic for this connection. You may also create a new virtual switch using the unclaimed network adapters listed below.

☒ **Create a virtual switch**

	Speed	Networks
<input type="checkbox"/> vmnic1	1000 Full	None
<input checked="" type="checkbox"/> vmnic2	1000 Full	None
<input checked="" type="checkbox"/> vmnic3	1000 Full	None

☐ **Use vSwitch0**

	Speed	Networks
<input type="checkbox"/> vmnic0	1000 Full	None

Preview:

VMkernel Port: VMkernel

Physical Adapters: vmnic2, vmnic3

≤ Back **Next >** Ca

- 5 Assign a Network Label. This label must be unique on the ESXi host being configured. Click **Next**.
In this example, the Network Label is "iSCSI1".

Port Group Properties

Network Label: **iSCSI1**

VLAN ID (Optional): None (0)

☐ Use this port group for vMotion

☐ Use this port group for Fault Tolerance logging

☐ Use this port group for management traffic

Preview:

VMkernel Port: iSCSI1

Physical Adapters: vmnic2, vmnic3

≤ Back **Next >** Cancel

- 6 Assign an IP address and subnet information for the first vmk port and click **Next**.
This example uses a static IP of 192.168.41.11 and a subnet mask of 255.255.255.0.

☐ Obtain IP settings automatically

☒ Use the following IP settings:

IP Address: 192 , 168 , 41 , 11

Subnet Mask: 255 , 255 , 255 , 0

VMkernel Default Gateway: 192 , 168 , 43 , 1 **Edit...**

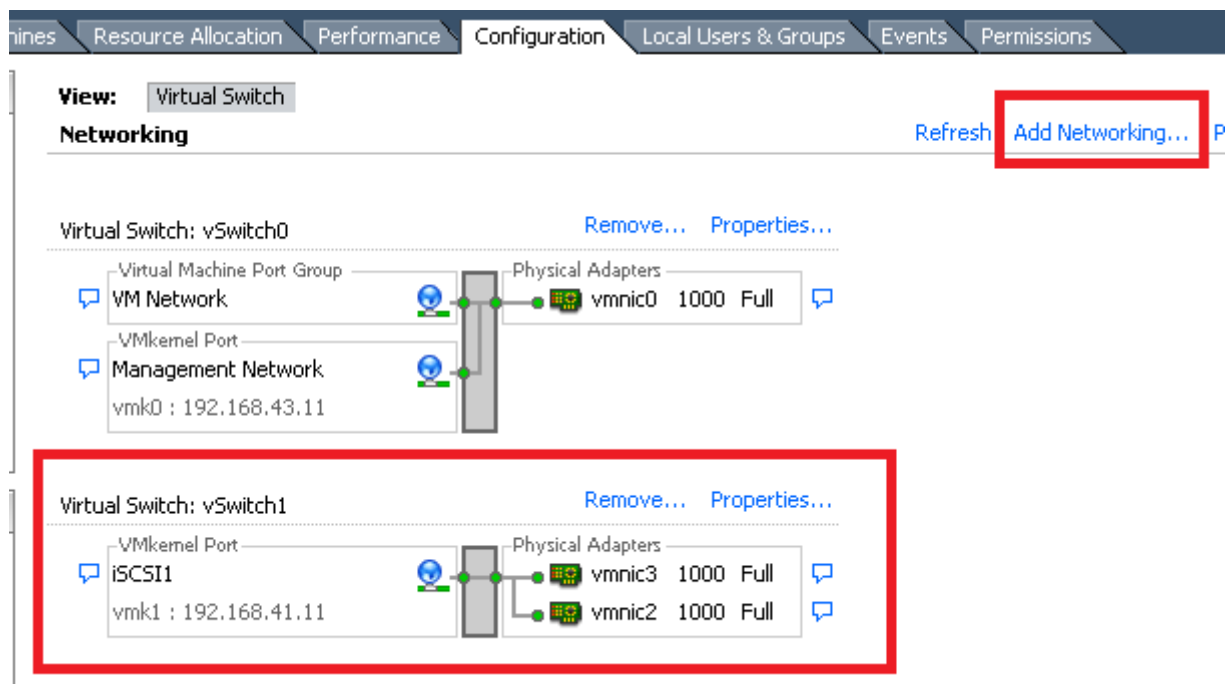
Preview:

VMkernel Port: iSCSI1
192.168.41.11

Physical Adapters: vmnic2, vmnic3

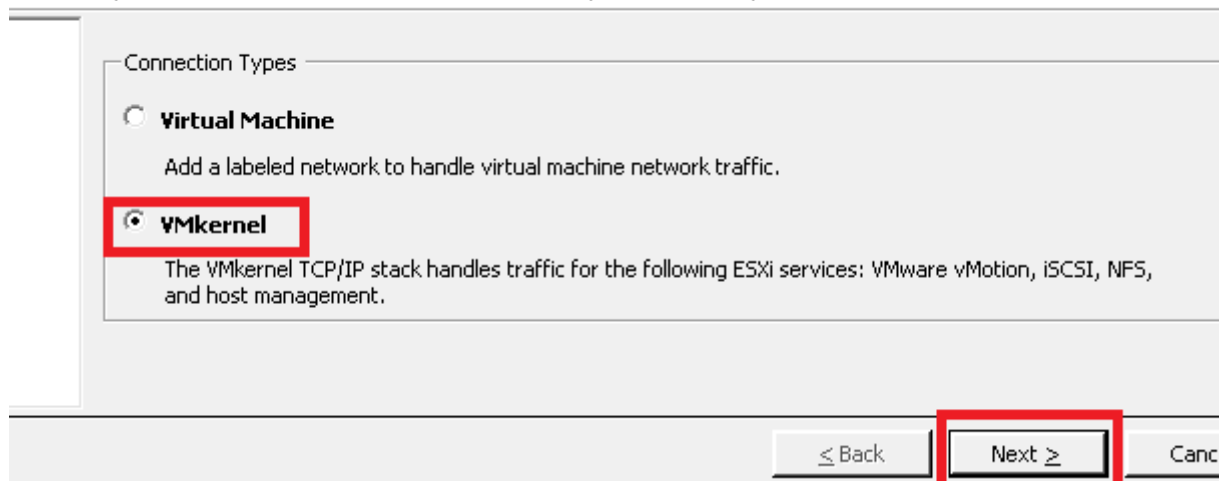
≤ Back **Next >** Cancel

- 7 Review the proposed configuration and if everything is correct, click **Finish**.
The Configuration / Networking screen is updated and displays the new vSwitch and vmk port.
- 8 To start configuring the second vmk port, click **Add Networking**.



9 Select VMkernel and click Next.

are can be partitioned to accommodate each service that requires connectivity.



10 Select the vSwitch that you created earlier and click Next.

This example uses *vSwitch1*.

cess

networks through uplink adapters attached to virtual switches.

Select which virtual switch will handle the network traffic for this connection. You may also create a new virtual switch using the unclaimed network adapters listed below.

<input type="radio"/> Create a virtual switch	Speed	Networks
<input type="checkbox"/> vmnic1	1000 Full	None
<hr/>		
<input type="radio"/> Use vSwitch0	Speed	Networks
<input type="checkbox"/> vmnic0	1000 Full	None
<hr/>		
<input checked="" type="radio"/> Use vSwitch1	Speed	Networks
<input checked="" type="checkbox"/> vmnic3	1000 Full	None
<input checked="" type="checkbox"/> vmnic2	1000 Full	None
<hr/>		

Preview:

The diagram shows two VMkernel ports on the left: 'VMkernel' and 'iSCSI1' (with IP address 'vmk1 : 192.168.41.11'). These are connected to a central vertical line representing a switch. On the right, two physical adapters are shown: 'vmnic3' and 'vmnic2'. The connections are as follows: 'VMkernel' connects to 'vmnic3', 'iSCSI1' connects to 'vmnic2', and both 'vmnic3' and 'vmnic2' are connected to the central switch line.

≤ Back **Next ≥** Can

11 Assign a Network Label and click Next.

The label must be unique on the ESXi host being configured. In this example, the Network Label is "iSCSI2".

Port Group Properties

Network Label:

VLAN ID (Optional):

☐ Use this port group for vMotion

☐ Use this port group for Fault Tolerance logging

☐ Use this port group for management traffic

Preview:

VMkernel Port: iSCSI2

VMkernel Port: iSCSI1

vmk1 : 192.168.41.11

Physical Adapters: vmnic3, vmnic2

≤ Back **Next ≥** Cancel

12 Assign an IP address and subnet information, then click **Next**.

This example uses a static IP of 192.168.41.111 and a subnet mask of 255.255.255.0.

tion Settings

settings

☐ Obtain IP settings automatically

☒ Use the following IP settings:

IP Address: 192 , 168 , 41 , 111

Subnet Mask: 255 , 255 , 255 , 0

VMkernel Default Gateway: 192 , 168 , 43 , 1 Edit...

Preview:

VMkernel Port

iSCSI2
192.168.41.111

VMkernel Port

iSCSI1
vmk1 : 192.168.41.11

Physical Adapters

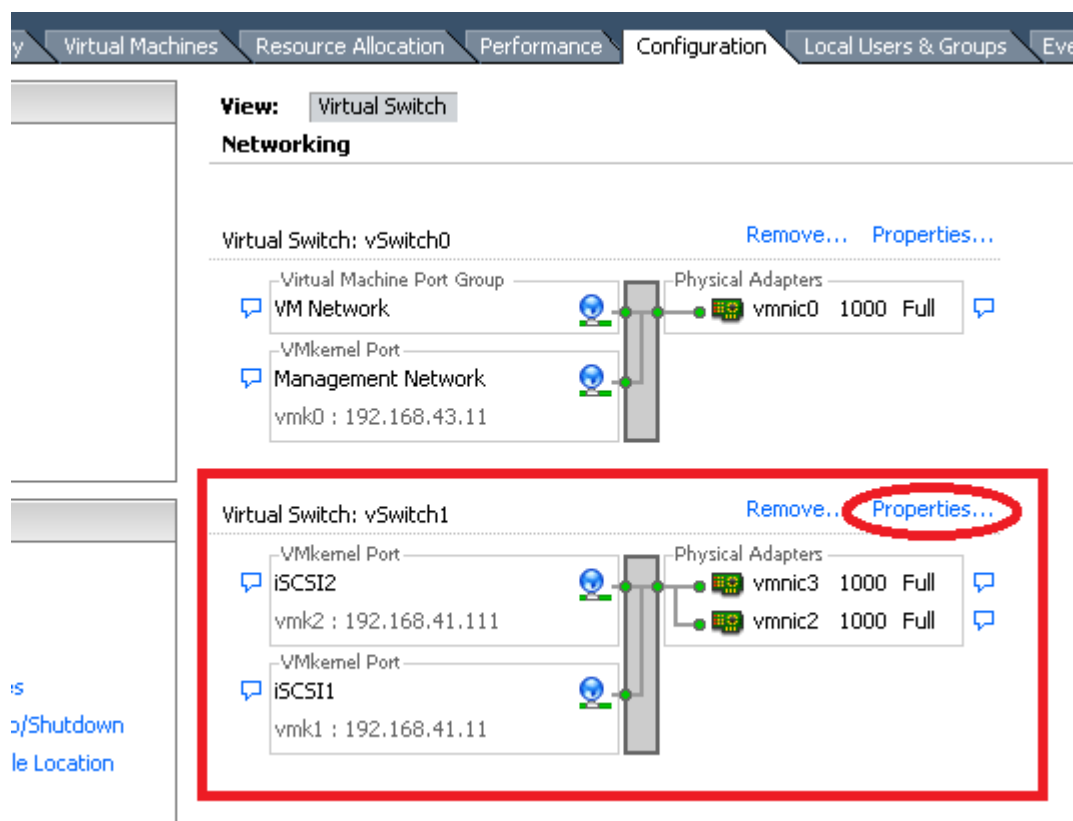
vmnic3
vmnic2

≤ Back Next ≥

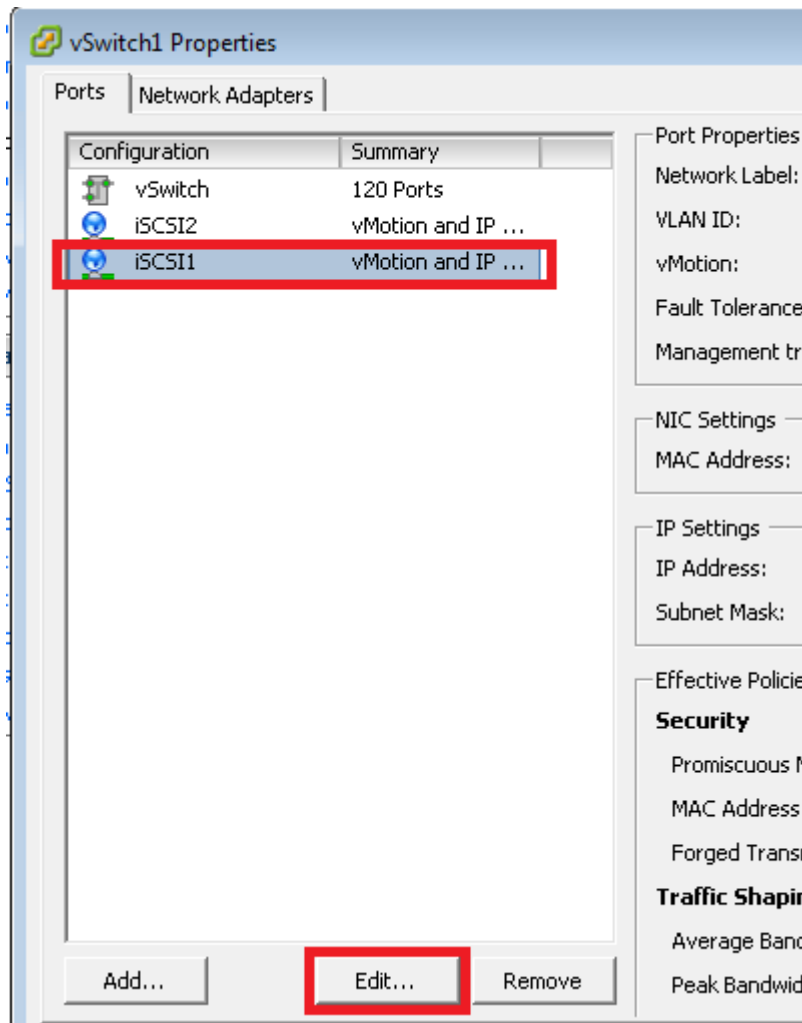
- 13** Review the proposed configuration and if everything is correct, click **Finish**.

The Configuration / Networking screen is updated and displays the new vSwitch and vmk ports. Note which vmk port is associated with each network label. In this example, the relationships are vmk1 = iSCSI1 and vmk2 = iSCSI2.

- 14** To disable NIC Teaming, click **Properties** on the vSwitch.



- 15 Select the first port group/network label and click **Edit**.
This example uses "iSCSI1".



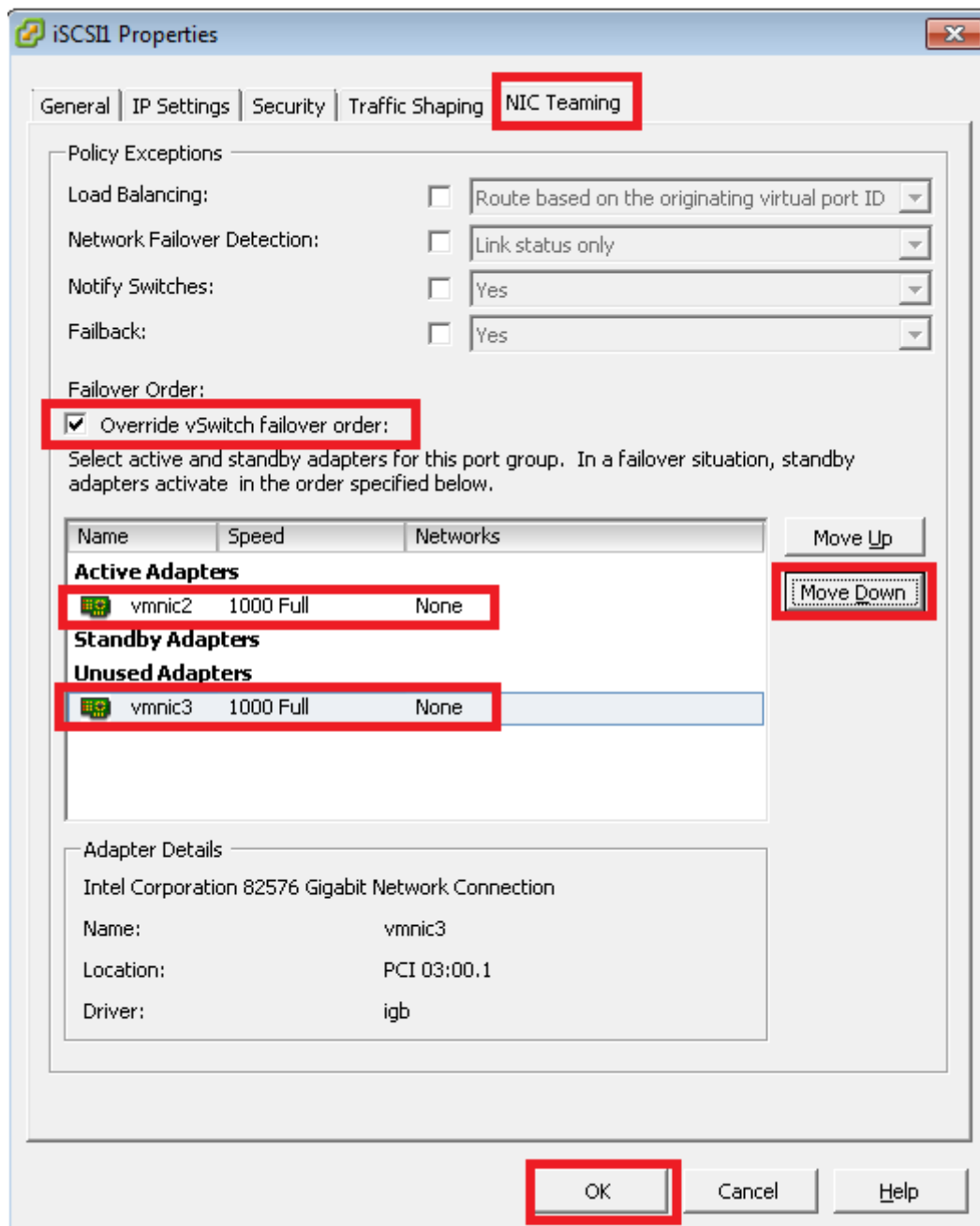
- 16** Go to the NIC Teaming tab, and check **Override vSwitch failover order**.

This example maps vmk1 (represented by the network label iSCSI1) to vmnic2.

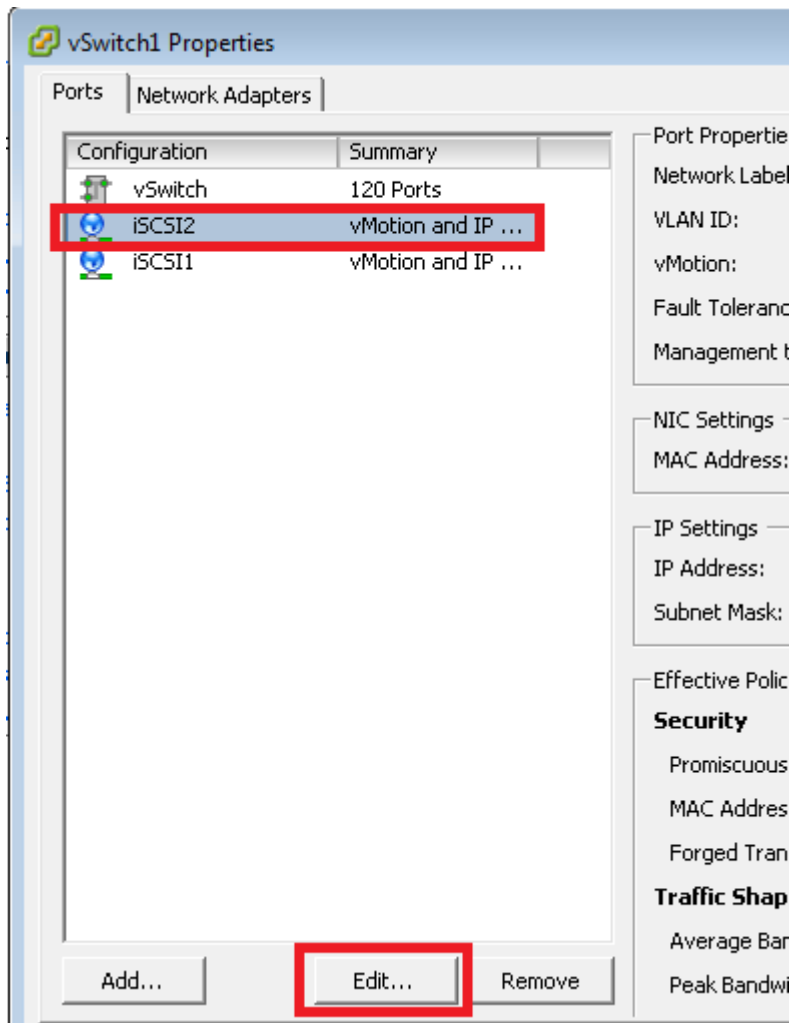
Click **OK** to finish.

- 17** Select the vmnic NOT to be used and click the **Move Down** button until that vmnic appears in the Unused Adapters section, then click **OK**.

In this example, vmic3 is not used, so it moves to the Unused Adapters section.



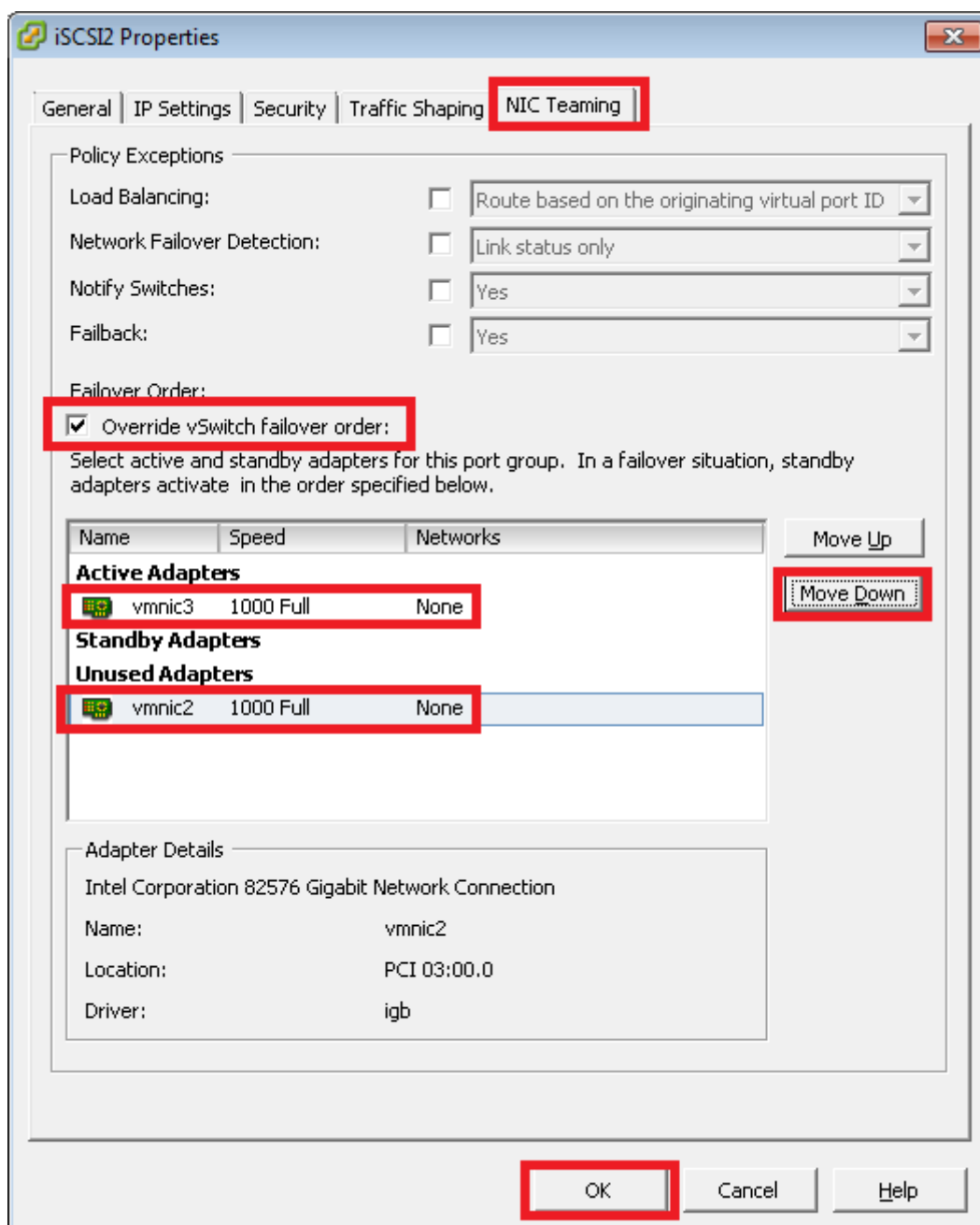
- 18** Select the second port group/network label and click **Edit**.
This example uses "iSCSI2".



19 Go to the NIC Teaming tab, and check **Override vSwitch failover order**.

20 Select the vmnic NOT to be used and click the **Move Down** button until that vmnic appears in the Unused Adapters section, then click **OK**.

In this example, vmic2 is not used, so it moves to the Unused Adapters section.



21 Click **Close**.

What to do next

Next, go to [Configure the ESXi iSCSI Software Adapter](#) on page 27.

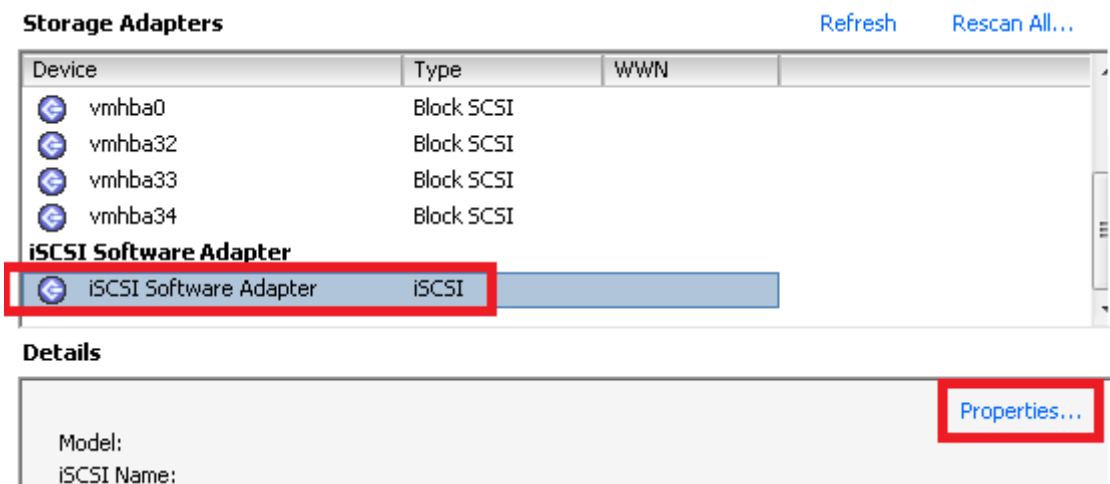
Configure the ESXi iSCSI Software Adapter

This procedure shows how to configure the ESXi iSCSI Software Adapter.

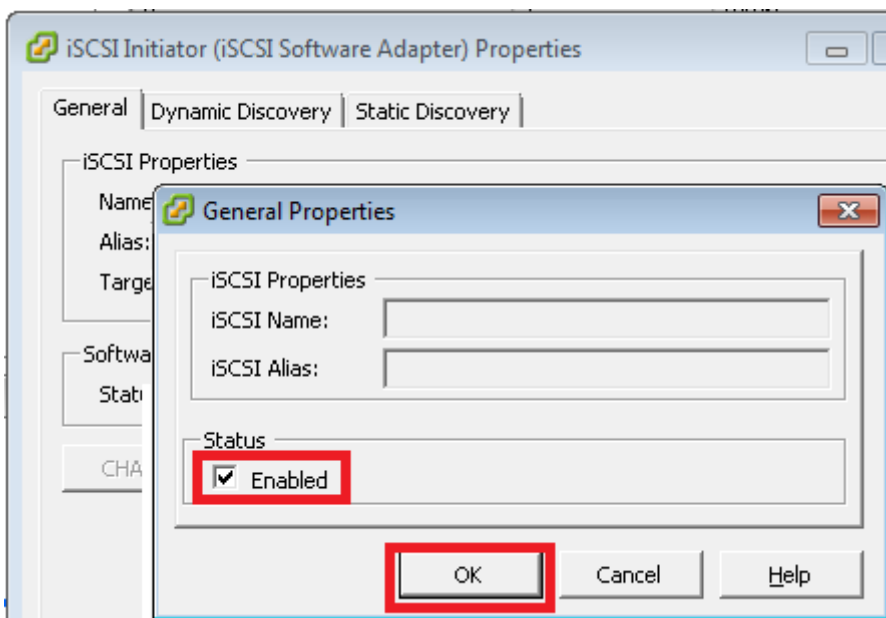
Procedure

- 1 Go to the Configuration / Storage Adapters screen on the ESXi host.

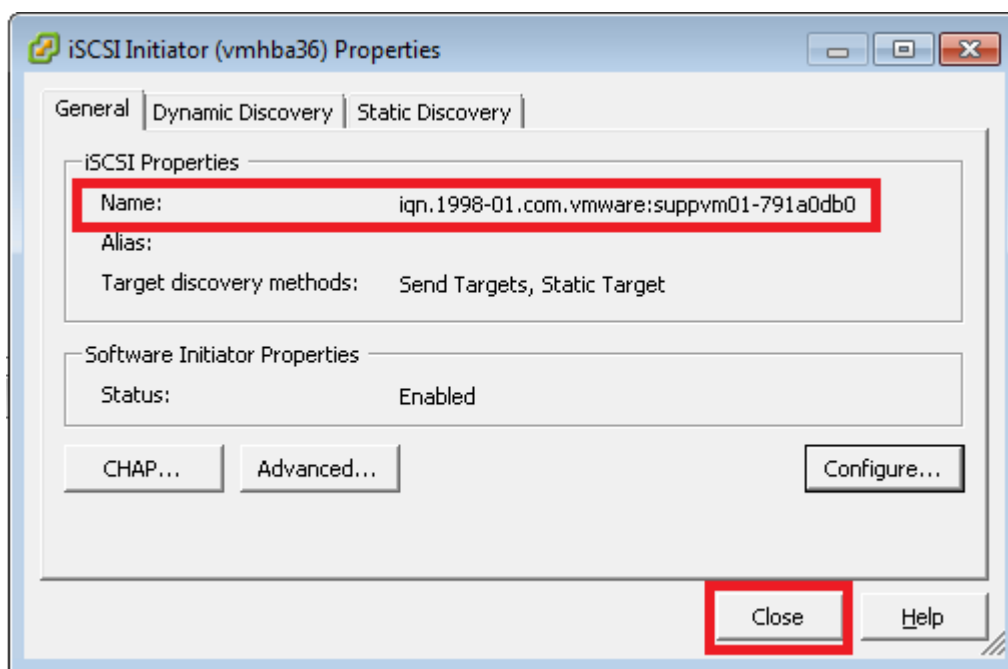
- 2 Scroll down, select the iSCSI Software Adapter, then click **Properties**.



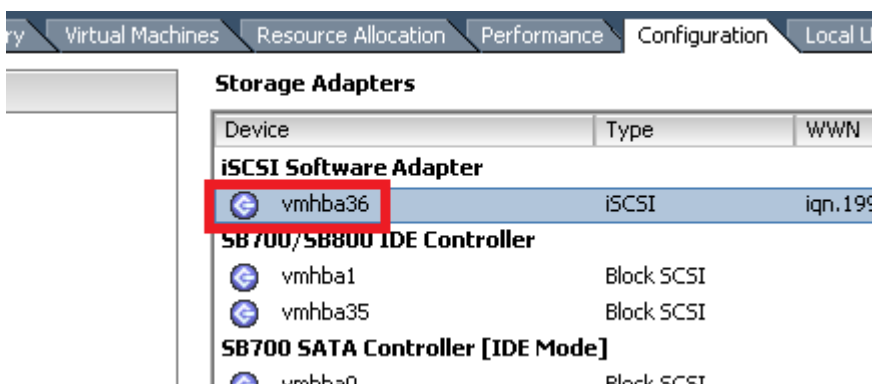
- 3 Click **Configure**.
- 4 Check **Enabled** then click **OK**.



- 5 Verify that the iSCSI initiator now has a name, then click **Close**.



- 6 Make a note of the vmhba## name of the iSCSI Software Adapter, where ## is a two-digit number. In this example, it is "vmhba36". You will use this name in the next task.



What to do next

Next, go to [Bind VMK Ports to ESXi iSCSI Software Adapter \(ESXi 5.0, 5.1, 5.5, 6.0, and 6.5\)](#) on page 29.

Bind VMK Ports to ESXi iSCSI Software Adapter (ESXi 5.0, 5.1, 5.5, 6.0, and 6.5)

This section applies to ESXi 5.0, 5.1, 5.5, 6.0, and 6.5 only. This action is required to ensure that all intended vmk and vmnic ports are used for I/O.

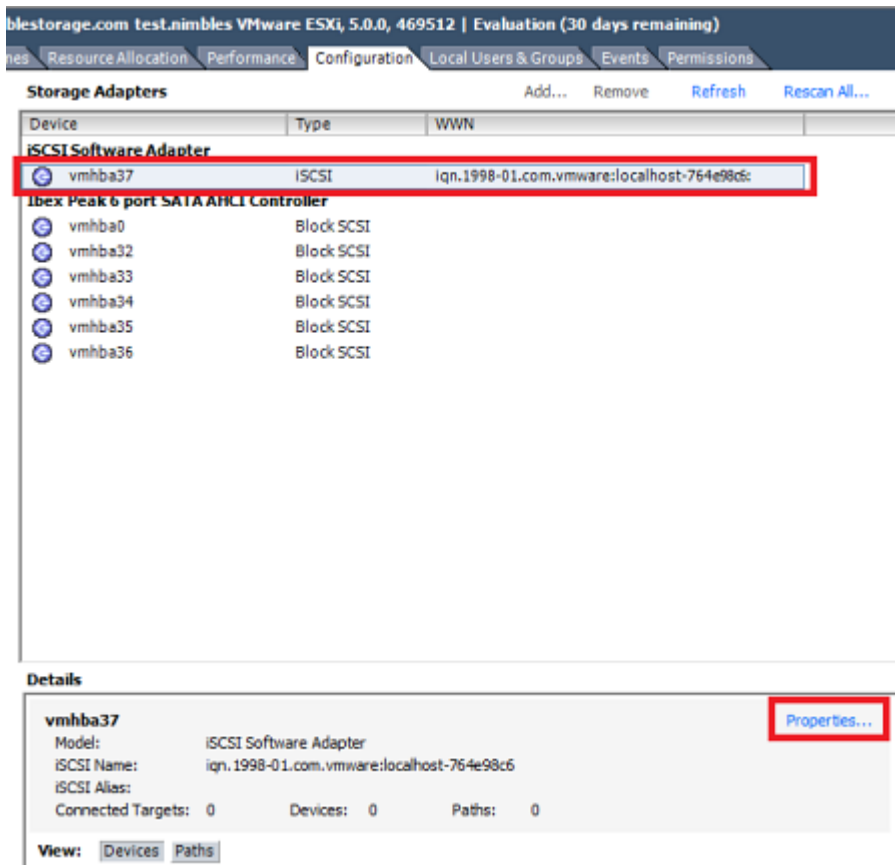
Note Nimble Connection Manager (NCM) does not support ESXi versions earlier than 5.0.

Important It is recommended to use port binding when all VMK ports for iSCSI reside in the same broadcast domain and IP subnet. If the VMK ports that are used for iSCSI are in a different broadcast domain and IP subnet, avoid using port binding. For more information, see

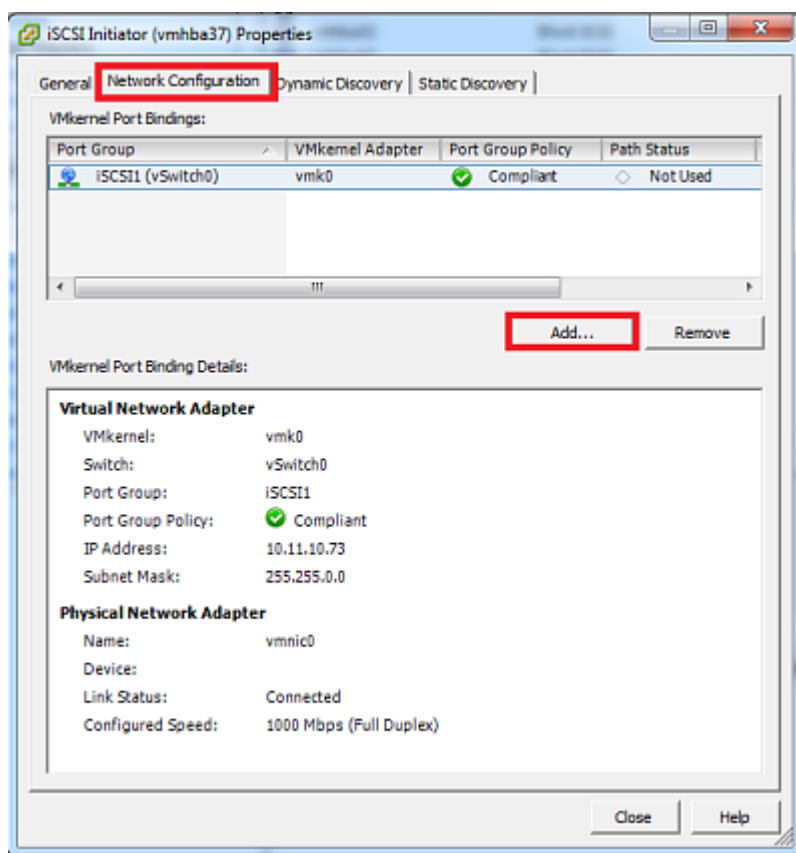
https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2038869

Procedure

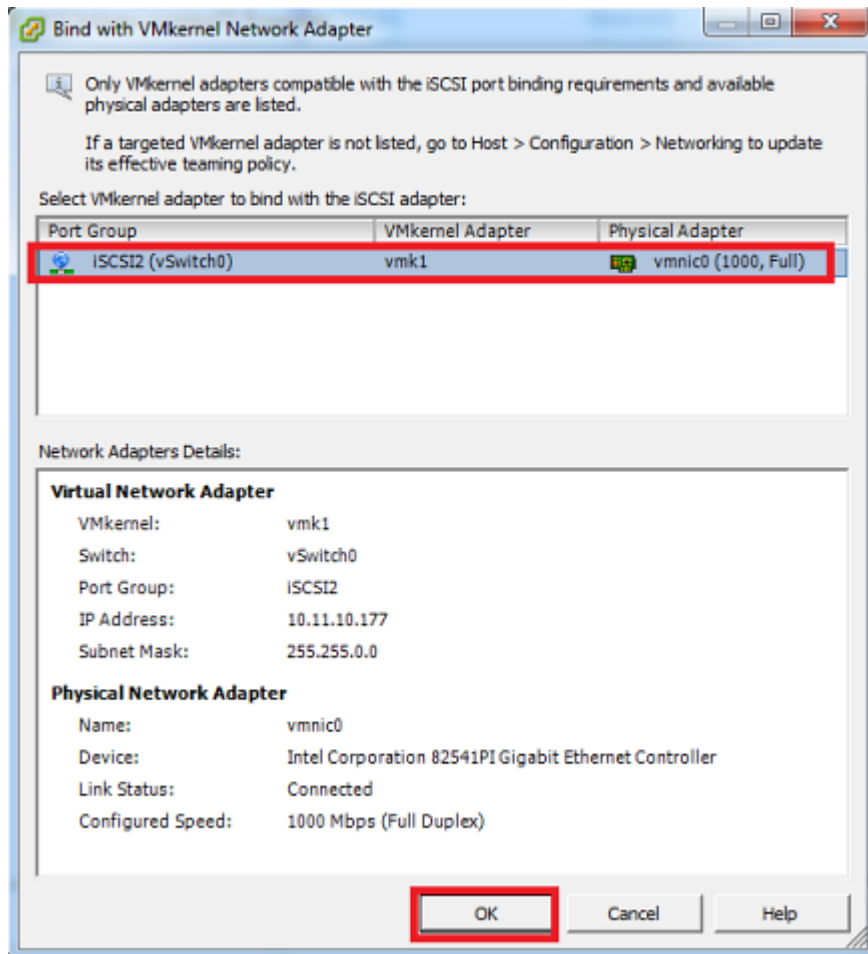
- 1 From the Configuration / Storage Adapters screen on the ESXi host, select the iSCSI Software Adapter and click **Properties**.



- 2 Tab to Network Configuration and click **Add**.



- 3 Select a vmk port used for iSCSI traffic and click **OK** to add it to the list.



4 Repeat the previous step for every vmk port used for iSCSI.

Note Ports can only be added one at a time.

5 Highlight any listed ports that are not used for iSCSI traffic, and click **Remove**.

6 Verify that the final list contains all of the vmk ports used for iSCSI traffic and no other ports.

What to do next

Next, go to [Nimble Connection Manager \(for iSCSI\)](#).

Nimble Connection Manager

The Nimble Connection Manager (NCM) manages connections from the host to volumes on Nimble systems. To simplify configuring multiple connections and Multipath Input/Output (MPIO), the NimbleOS requires that only one IP address (the iSCSI discovery IP address) be advertised, instead of needing to advertise the full set of iSCSI network interfaces at the time of discovery.

This means that you do not need to manually make specific connections to the appropriate interfaces, or worry about how many connections there are to a volume. As connections are made to the same address (group target portal), the connections are redirected to the appropriate distribution of actual iSCSI network interfaces.

Understand the Nimble Connection Manager

Prior to NimbleOS 2.0, volumes always resided on a single Nimble array. Beginning with NimbleOS 2.0 and the introduction of storage groups and pools, volumes can now span multiple arrays that are grouped into storage pools. A host can no longer assume that the volume is fully accessible from one specific array. An I/O request sent to the wrong array must be forwarded to the correct array, resulting in a decrease in I/O performance.

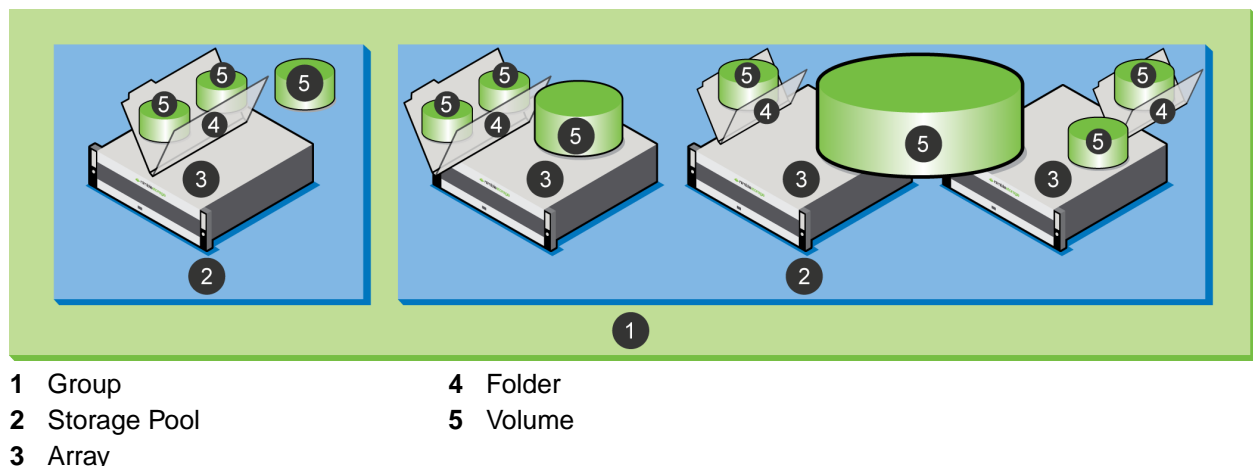
Group

A group (sometimes referred to as a cluster) is a set of member arrays that are physically connected and logically represent a single storage entity for the purposes of aggregating performance, capacity and simplifying management. For most administrative tasks, a group looks and feels very much like a single array. A group contains one or more disjoint pools.

A group is a collection of one to four Nimble arrays. You interact with the group by connecting to its management IP address, hosted by one of the arrays in the group. Data is striped across the arrays in the same pool. From the perspective of the user, the group looks and acts like a single array.

You can also remove an array from a group provided the array is not part of any pools in the group. You can only remove an array when the remaining arrays in the group have enough space for the data in the array being removed.

Figure 1: Relationships of Groups, Pools, Arrays, Folders, and Volumes in Multi-array Groups



Pool

A pool confines data to a subset of the arrays in a group. Data of resident volumes is striped and automatically rebalanced over the members of the group. Pools are important to the extent that they dictate physical locality and striping characteristics. It might be easier to think of a pool as a logical container that contains one or more member arrays in which volumes reside. A member array can only be a part of one pool.

- Volumes and their respective snapshots and clones reside within a pool and are tied to a specific pool.
- You can migrate volumes between different pools.
- Volume collections are not tied to pools and can contain volumes that reside in different pools.

Nimble Connection Manager

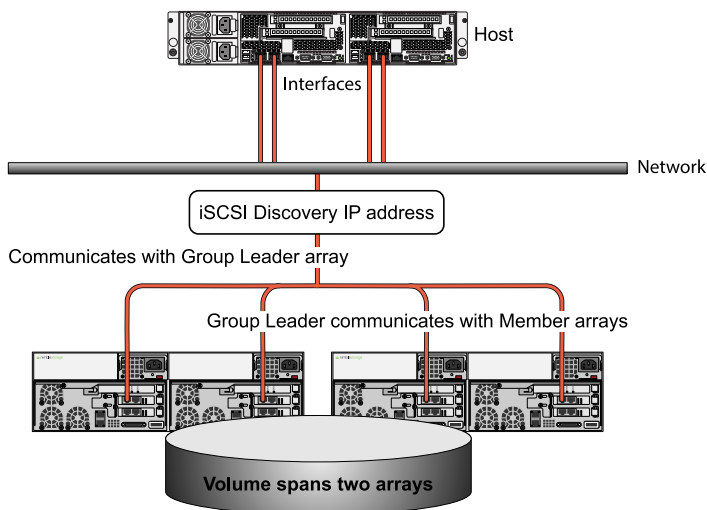
Nimble Connection Manager (NCM) consists of two components:

Component	Function
Nimble Connection Service (NCS)	NCS automatically calculates and maintains the optimal number of iSCSI sessions from the host to the storage group balanced across the host NICs for a Nimble Storage device.
Nimble Path Selection Plugin (PSP)	The PSP for VMware Pluggable Storage Architecture automatically directs the I/O request for a Nimble Storage device to the most favorable route.

If you add an array to a storage group, the volume may be adjusted and balanced to reside partially on the newly added array. In this case, Nimble Connection Manager automatically creates the optimal number of connections to the array.

Within the storage group, through the group leader array, Nimble PSP determines how many and on which arrays the volume resides and redirects communication to the appropriate paths.

Figure 2: NCM Diagram



All of this ensures that even with arrays being added or removed from a storage group, the correct number of connections are made without the need for ongoing manual configuration.

Best Practice

Nimble recommends using NCM for automatic iSCSI session management and achieving optimal I/O performance on Nimble devices.

NCM Installation

Nimble Connection Manager (NCM) is a package available on the Nimble InfoSight Software downloads site. NCM is installed on the ESXi host. After installation, the Nimble Connection Service (NCS) and Nimble Path Selection Plugin (PSP) begin to function immediately.

This document describes installation using vSphere Update Manager or the ESXCLI utility on the ESXi host. You can also use the vCLI utility from a Windows or Linux host. See your VMware documentation for more information.

Prerequisites to NCM Installation

System prerequisites:

- ESXi 5.0, 5.1, 5.5, 6.0, or 6.5 with the VMware vSphere Standard, Enterprise or Enterprise Plus licensing running on the host

Note The Standard license applies to VMware vSphere 6 and later.

- vCenter Server 5.0, 5.1, 5.5, 6.0, or 6.5

Before copying and installing the NCM package, you must:

- Determine which version of ESXi host and NCM you want to use:
 - If you are using ESXi 5.0, 5.1, or 5.5, use NCM for ESXi 5.
 - If you are using or updating to ESXi 6.0, use NCM for ESXi 6.
 - If you are using or updating to ESXi 6.5, use NCM for ESXi 6.5.

To use ESXi 6.0:

- Upgrade the ESXi host to 6.0.
- Uninstall your current NCM installation.
- Install NCM for ESXi 6.

To use ESXi 6.5:

- Upgrade the ESXi host to 6.5.
- Uninstall your current NCM installation.
- Install NCM for ESXi 6.5.

Additional prerequisites:

- Internet connection to the Windows or Linux host
- Login ID and password for the Nimble Storage InfoSight software downloads site
- SFTP client on the Windows or Linux host, such as WinSCP
- SSH client on the Windows or Linux host, such as PuTTY
- Root access to the ESXi host
- A 15-minute interval when your ESXi host can be offline

If an ESXi host is connected to at least one array running NimbleOS 2.x or later, install NCM.

If an ESXi host is connected to both NimbleOS 1.x and 2.x arrays, it is recommended that you install NCM. NCM actively manages iSCSI connections for volumes from 2.x arrays, but it does not manage volumes from 1.x arrays.

Important NCM cannot be installed on ESXi hosts that are in lockdown mode. You must first disable lockdown mode before installing NCM. For more information see [VMware KB article 1008077](#).

NCM Installation Methods

NCM can be installed on the ESXi host by using either the ESXCLI or the vSphere Update Manager. These options can be used when ESXi has Internet connectivity and even when it cannot connect to the Internet.

Note The preferred installation method is to use the vSphere Update Manager.

Tool	Internet Connection	Procedure
vSphere Update Manager	Online	vSphere Update Manager automatically downloads and installs the NCM bundle. See Install NCM When vCenter Has Internet Connection on page 38.
	Offline	Manually download the NCM bundle to a Windows or Linux host, and install it using vSphere Update Manager. See Install NCM When vCenter Has No Internet Connection on page 39.
ESXCLI	Online	Automatically downloads and installs the NCM bundle with a single ESXCLI command. The ESXi host must have Internet access to the Nimble Storage support site. See Install NCM Online Bundle Through ESXCLI on page 41.
	Offline	Download the NCM bundle to a Windows or Linux host, copy the bundle to the ESXi host, and install the bundle using the ESXCLI utility. See Install NCM Offline Bundle Through ESXCLI on page 42.

Copy NCM to the ESXi Host

Before you begin

Note If you are updating NCM to version 6.0 or 6.5, you must first update the ESXi host to 6.0 or 6.5, then uninstall your current NCM installation.

To install NCM using the ESXCLI utility, you must:

- Have an SFTP client on the Windows or Linux host, such as WinSCP
- Download the NCM installation package from the Nimble Support site
- Have root access to the ESXi host
- Reboot after NCM installation if updating to NCM 6.0.
- Reboot after NCM installation if updating to NCM 6.5.

Note It is not necessary to reboot if you are installing NCM for the first time.

Procedure

- 1 Launch your SFTP client on the Windows or Linux host.
- 2 Type the IP address of the ESXi server into the Host name: field, **root** in the user name field, and your password into the password field, then click **Login**.

- 3 Drag the icon of the NCM installation package (filename `nimble-ncm-x.x.x-xxxxxxx.zip`) from the Windows server to the `/tmp` directory on the ESXi host.

Note If updating to NCM 6.0 or 6.5, be sure to download the corresponding 6.0 or 6.5 version of the installation package.

- 4 Click the X icon in the top right corner of the window to close the SFTP client.

Install NCM When vCenter Has Internet Connection

The installation procedure for NCM is the same for ESXi 5.0, 5.1, 5.5, 6.0, and 6.5.

Before you begin

To install the Nimble Connection Manager (NCM) using the Update Manager when the vCenter server has an Internet connection, you must have:

- vSphere Update Manager installed on the vCenter server
- Root access to the ESXi host
- A 15-minute interval when your ESXi host can be offline

For more information, see *Installing and Administering VMware vSphere Update Manager*.

Note `update.nimblestorage.com` requires TLS v1.2 or later support on the host.

Procedure

- 1 On the vSphere client Home screen, click the **Update Manager** icon.
- 2 On the Configuration tab, click **Download Settings**.
- 3 Click **Add Download Source**, and enter one of these source URLs, then click **OK**.
 - For ESXi 5.0, 5.1, or 5.5:
`https://update.nimblestorage.com/esx5/ncm/index.xml`
 - For ESXi 6.0:
`https://update.nimblestorage.com/esx6/ncm/index.xml`
 - For ESXi 6.5:
`https://update.nimblestorage.com/esx6.5/ncm/index.xml`
- 4 Click **Download Now** to upload the package, then click **Apply**.
- 5 Click the **Baselines and Groups** tab, look for the Baselines list, and then click **Create...**
- 6 Type `ncm baseline` in the Name field, choose the **Host Extension** option, and then click **Next**.
vCenter refers to a collection of patches to be installed a baseline.
- 7 In the Extensions pane, click the down arrow to move the Nimble installation package to the Extensions to Add list, click **Next** and then click **Finish**.
- 8 Click **Compliance View**, click the datacenter for your ESXi hosts, and on the Update Manager tab, and then click **Attach...**
- 9 In the Attach Baseline or Group dialog box, check the **ncm baseline** box and then click **Attach**.
- 10 On the Update Manager tab, select the ESXi hosts where you want to install NCM and click **Scan...**
The scan shows that the baseline is *non-compliant*, meaning that the baseline has not yet been applied to the ESXi host.
- 11 Click **Stage** to prepare the baseline for installation, click **Next** and then click **Finish**. Wait until the stage action is complete.

12 Click **Remediate** to apply the baseline to the ESXi host, click **Next** and enter a Task Description and click **Next**, and then click **Finish**.

Results

After the installation:

- Nimble Connection Service (NCS) automatically creates the optimal number of sessions for each Nimble volume.
- Nimble Path Selection Plugin (PSP) automatically claims the available Nimble devices, including both existing devices and devices added later.

For most applications, NCS and PSP require no configuration.

What to do next

Go to [Verify NCM Installation](#) on page 43.

Install NCM When vCenter Has No Internet Connection

Installing NCM with no Internet connection is known as an *offline bundle* installation.

Note The installation procedure for NCM is the same for ESXi 5.0, 5.1, 5.5, 6.0, and 6.5.

Before you begin

To install the Nimble Connection Manager (NCM) on all hosts at once using the Update Manager, you must have:

- The downloaded NCM installation package
See [Download the NCM Installation Package](#) on page 40
- vSphere Update Manager installed on the vCenter server
- Root access to the ESXi host
- A 15-minute interval when your ESXi host can be offline

For more information, see *Installing and Administering VMware vSphere Update Manager*.

Procedure

- 1 On the vSphere client Home screen, click the **Update Manager** icon.
- 2 On the Configuration tab, click **Download Settings**.
- 3 Click **Import Patches**, select the Nimble installation package, and click **OK**.
vCenter refers to the Nimble installation package as a *patch*.
- 4 Click **Next** to upload the package, then click **Finish**.
- 5 Click the Baselines and Groups tab, look for the Baselines list, then click **Create....**
- 6 Type **ncm baseline** in the Name field, choose the Host Extension option, and click **Next**.
vCenter refers to a collection of patches to be installed as a *baseline*.
- 7 In the Extensions pane, click the down arrow to move the Nimble installation package to the Extensions to Add list, click **Next**, then click **Finish**.
- 8 Click **Compliance View**, click the datacenter for your ESXi hosts, and on the Update Manager tab, then click **Attach....**
- 9 In the Attach Baseline or Group dialog box, check the **ncm baseline** box, then click **Attach**.
- 10 On the Update Manager tab, select the ESXi hosts where you want to install NCM and click **Scan....**
The scan shows that the baseline is *non-compliant*, meaning that the baseline has not yet been applied to the ESXi host.

11 Click **Stage** to prepare the baseline for installation, click **Next**, then click **Finish**.

Note Wait until the stage action is complete before proceeding.

12 Click **Remediate** to apply the baseline to the EXSi host, click **Next**, type a Task Description, click **Next**, then click **Finish**.

Results

After the installation:

- Nimble Connection Service (NCS) automatically creates the optimal number of iSCSI sessions for each Nimble volume.
- Nimble Path Selection Plugin (PSP) automatically manages the selection of paths to the volumes.

For most applications, NCS and PSP require no configuration.

What to do next

Go to [Verify NCM Installation](#) on page 43.

Download the NCM Installation Package

Follow this procedure to install NCM as an *offline bundle*.

Before you begin

To download the Nimble Connection Manager (NCM) installation package, which is an offline bundle, you must have:

- Internet connection to the Windows or Linux host
- User name and password for the Nimble Storage InfoSight portal

You can obtain a user name and password at the portal. Click **New user? Enroll now** and supply the requested information.

Procedure

- 1 In your Internet browser, go to <https://infosight.nimblestorage.com/>.
- 2 Enter your log in ID and password, then click **Login**.
- 3 Choose **Resources > Software Downloads**.
- 4 Under **Integration Kits**, click Connection Manager (NCM) for VMware.
- 5 In the Current Version list, click one of the **Downloads** packages.

Note If updating to NCM 6.0 or 6.5, be sure to download the corresponding 6.0 or 6.5 version of the installation package.

- 6 Save the NCM installation package to a convenient place on your Windows server.
The installation package name is in the format `nimble-ncm-x.x.x-xxxxxx.zip` where `x.x.x` is the version number and `xxxxxx` is the build number.

Note Do not unzip the installation package.

- 7 (Optional) Download the latest version of the *Nimble Connection Manager for VMware Release Notes*.

What to do next

Install NCM using one of the following methods:

- [Install NCM When vCenter Has No Internet Connection](#) on page 39

- [Install NCM Offline Bundle Through ESXCLI](#) on page 42

Install NCM Online Bundle Through ESXCLI

You can install Nimble Connection Manager (NCM) on the ESXi host as an *online bundle* from the Nimble Storage InfoSight software download portal. In this case, the NCM bundle does not need to be downloaded and copied to the ESXi host. However, the ESXi host must have access to the Internet in order to access the URL.

Before you begin

System prerequisites:

- NimbleOS 2.x or later running on the Nimble array
- ESXi 5.0, 5.1, 5.5, 6.0, or 6.5 running on the ESXi host
- vCenter Server 5.0, 5.1, 5.5, 6.0, or 6.5

Additional prerequisites:

- Copy NCM onto the ESXi host.
- The ESXi host must have Internet access to the Nimble Storage Support site.
- You must have an SSH client on the Windows or Linux host, such as PuTTY.
- You must have root access to the ESXi host.

Note update.nimblestorage.com requires TLS v1.2 or later support on the host.

Procedure

- 1 Place the ESXi host in maintenance mode using the vSphere Client (web-based or desktop) plugin.
- 2 Launch your SSH client on the Windows or Linux host.
- 3 Type the IP address of the ESXi server into the Host name: field; then click **Open**.
- 4 Log into the ESXi host as the root user.
- 5 Run one of the following commands from the root directory to install the online NCM bundle.

- For ESXi 5.0, 5.1, or 5.5 enter:

```
esxcli software vib install -d https://update.nimblestorage.com/esx5/ncm
```
- For ESXi 6.0, enter:

```
esxcli software vib install -d https://update.nimblestorage.com/esx6/ncm
```
- For ESXi 6.5, enter:

```
esxcli software vib install -d https://update.nimblestorage.com/esx6.5/ncm
```

Note You must reboot the ESXi host whenever you update or uninstall NCM or whenever you do a fresh install of NCM on ESXi 6.0 or 6.5. However, a fresh install of NCM on ESXi 5.0, 5.1, or 5.5 does not require a reboot.

Results

After the installation:

- Nimble Connection Service (NCS) automatically creates the optimal number of iSCSI sessions for each Nimble volume.
- Nimble Path Selection Plugin (PSP) automatically manages the selection of paths to each Nimble volume.

For most applications, NCS and PSP require no configuration.

What to do next

Go to [Verify NCM Installation](#) on page 43.

Install NCM Offline Bundle Through ESXCLI

This method is also known as an *offline bundle* installation.

Note The installation procedure for NCM is the same for ESXi 5.0, 5.1, 5.5, 6.0, and 6.5.

Before you begin

To install the Nimble Connection Manager (NCM) offline bundle using the ESXCLI utility, you must have:

- The downloaded NCM installation package
See [Download the NCM Installation Package](#) on page 40
- An SSH client on the Windows or Linux host, such as PuTTY
- Root access to the ESXi host

Procedure

- 1 Place the ESXi host in maintenance mode using the vSphere Client (web-based or desktop) plugin.
- 2 Launch your SSH client on the Windows or Linux host.
- 3 Type the IP address of the ESXi server into the Host name: field, then click **Open**.
- 4 Log into the ESXi server as the root user.
- 5 From the root directory, run the command:

```
esxcli software vib install -d /tmp/ncm_2-1-0-0_nimble-ncm-x.x.x-xxxxxx.zip
```

Where **x.x.x** is the version number and **xxxxxx** is the build number of the NCM installation package.

Note If updating to NCM 6.0 or 6.5, be sure to install the corresponding 6.0 or 6.5 version of the installation package.

Important

- Type the absolute path to the NCM download; do not use a relative path.
- Do not use any spaces or special characters in the path.

Note You must reboot the ESXi host whenever you update or uninstall NCM or whenever you do a fresh install of NCM on ESXi 6.0 or 6.5. However, a fresh install of NCM on ESXi 5.0, 5.1, or 5.5 does not require a reboot.

Results

After the installation:

- Nimble Connection Service (NCS) automatically creates the optimal number of sessions for each Nimble volume.
- Nimble Path Selection Plugin (PSP) automatically claims the available Nimble devices, including both existing devices and devices added later.

For most applications, NCS and PSP require no configuration.

What to do next

Go to [Verify NCM Installation](#) on page 43.

Verify NCM Installation

Before you begin

To verify installation of NCM on the ESXi host, you must have an SSH client on the Windows or Linux host, such as PuTTY.

Procedure

- 1 Launch your SSH client on the Windows or Linux host.
- 2 Type the IP address of the ESXi host in the Host name: field, then click **Open**.
- 3 Log in to the ESXi host as the root user.
- 4 From the root directory, run the command:
esxcli software vib list | grep nimble
If *nimble-ncs* and *nimble-psp* appear in the list, the installation was successful.

Configure NCM on the ESXi Host

The configuration procedure for NCM is the same for ESXi 5.0, 5.1, 5.5, 6.0, and 6.5.

Note The default NCM configuration has been tested as suitable for most users. Do not change the NCM configuration unless you have specific reasons for doing so.

Before you begin

To view the Nimble Connection Manager (NCM) configuration, you must have an SSH client on the Windows server, such as PuTTY.

To change the NCM configuration, you must have:

- An SSH client on the Windows or Linux host, such as PuTTY
- A text editor, such as vi

Procedure

- 1 Launch your SSH client on the Windows or Linux host.
- 2 Type the IP address of the ESXi host in the Host name: field, then click **Open**.
- 3 Log in to the ESXi host as the root user.
- 4 From the root directory, change to the Nimble directory.
cd /etc/nimble/
- 5 From the `/etc/nimble/` directory, type **cat ncm.conf**.

The NCM configuration file displays.

Configuration Items and Default Values	Descriptions and Options
interval: 120	Interval refers to time in seconds.
min_volsessions: 2	The minimum number of iSCSI sessions to the ESXi server for each volume. The default is 2.
max_volsessions: 8	The maximum number of iSCSI sessions to the ESXi server for each volume. The default is 8.

Configuration Items and Default Values	Descriptions and Options
worker_stop: 0	0 allows the Nimble Connection Service (NCS) to monitor your sessions. 1 prevents the NCS from monitoring your sessions.

Note The valid range of values for *min_volsessions* and *max_volsessions* is from 2 to 32. If a value is specified outside this range, the NCS reverts the value to the default value.

- 6 (Optional) If you want to make changes to the configuration, open the `ncm.conf` file in a text editor.

View NCM Logs

The NCM logs can provide helpful troubleshooting information for a Nimble Storage Support engineer.

Before you begin

To view the Nimble Connection Manager (NCM) logs, you must have:

- An SSH client on the Windows or Linux host, such as PuTTY
- A text editor, such as vi

Procedure

- 1 Launch your SSH client on the Windows or Linux host.
- 2 Type the IP address of the ESXi host in the **Host name:** field, then click **Open**.
- 3 Log into the ESXi host as the root user.
- 4 From the root directory, change to the logs directory.

```
cd /var/log/nimble/
```

- 5 From the `/var/log/nimble/` directory, view the list of logs.

Is

The list of Nimble logs is displayed:

- `ncm.log`
- `nimble_psp_installer.log`
- `nimble_psp_policy.log`

- 6 To view individual logs, type **vi /var/log/nimble/xxx.log**, where `xxx` is the name of a specific log file.

Update NCM

When you update NCM on the ESXi host, you install a full version of NCM on top of an existing installation. You can install the update without uninstalling the current version of NCM.

You can use any installation method to install the NCM update:

- [Install NCM Online Bundle Through ESXCLI](#) on page 41
- [Install NCM Offline Bundle Through ESXCLI](#) on page 42
- [Install NCM When vCenter Has Internet Connection](#) on page 38
- [Install NCM When vCenter Has No Internet Connection](#) on page 39

Important After installing the update, you must reboot the ESXi host through the ESXi console or from the vSphere client. You must reboot the ESXi host whenever you update or uninstall NCM or whenever you do a fresh install of ESXi 6.0 or 6.5. However, a fresh install of NCM on ESXi 5.x does not require a reboot.

The reboot operation takes 10 to 15 minutes. When the reboot is complete, you must reestablish your SSH client connection.

Before you begin

To update Nimble Connection Manager (NCM), you must have:

- The downloaded NCM installation package
See [Download the NCM Installation Package](#) on page 40
- An SSH client on the Windows or Linux host, such as PuTTY
- Root access to the ESXi host
- A 15-minute interval when your ESXi host can be offline

Uninstall NCM

The only time you need to uninstall NCM from an ESXi host is if you plan to downgrade your array from NimbleOS 2.0 to NimbleOS 1.x.

Before you begin

To uninstall Nimble Connection Manager (NCM), you must have:

- An SSH client on the Windows or Linux host, such as PuTTY
- Root access to the ESXi host
- A 15-minute interval when your ESXi host can be offline

Procedure

- 1 Launch your SSH client on the Windows or Linux host.
- 2 Type the IP address of the ESXi host in the Host name: field, then click **Open**.
- 3 Log in to the ESXi host as the root user.
- 4 From the root directory, run the command:
/etc/init.d/sfcbd-watchdog stop
- 5 When the prompt reappears, run the command:
esxcli software vib remove -n nimble-ncs --maintenance-mode
- 6 When the prompt reappears, run the command:
esxcli software vib remove -n nimble-psp --maintenance-mode
- 7 Reboot the ESXi host through the ESXi console or from the vSphere client.
The reboot operation takes 10 to 15 minutes. When the reboot is complete, you must reestablish your SSH client connection.

VMware Synchronized Snapshots

NimbleOS contains built-in VMware integration that allows NimbleOS snapshots to be synchronized with VMware Virtual Machine snapshots in the VMFS datastore environment. Doing this ensures that they are application-consistent. To use this feature, no additional configuration is required in the guest OS; however, you must have the latest VMware Tools installed.

Because of this synchronized snapshots integration, NimbleOS lets you schedule and manage application-consistent snapshots and replicas. Synchronizing snapshots coordinates with the application to quiesce I/O to ensure that the snapshot does not capture in-progress writes. NimbleOS gives you the ability to coordinate with the VMware vCenter Server and VSS Services Support in VMware Tools by using vSphere APIs to quiesce I/O to ensure that the snapshot does not capture any in-progress file system transactions.

Note Nimble Storage supports VM-consistent snapshots for VVols and application-consistent snapshots for SQL and Exchange applications only.

To use VMware synchronized snapshots, select *VMware synchronization* for a volume collection and include the vCenter Server, an Administrator user name and password. The system works with vCenter to take application-consistent snapshots.

A vCenter synchronized snapshot can be scheduled in a volume collection. The system takes snapshots of all volumes in the volume collection at the same time. By using the vSphere APIs and VSS Services Support in VMware Tools, snapshots and replicas are application consistent, rather than just crash consistent. As a result, when you restore from a Nimble-based snapshot, the application can immediately start using the data without performing extra restore recovery steps.

For testing and development, a snapshot can be cloned instantly and used to verify an application's compatibility with the system or to use with a new application.

Nimble array clones are *zero-copy*: they share data blocks with the source volume, creating an extremely capacity- and time-efficient read/write copy for test or development purposes.

How Nimble Synchronization Works with VMware

Virtual Machines are in a datastore that is on the specified Nimble volume(s). When VMware synchronization is enabled in the volume collection, the software in the Nimble array communicates directly with vCenter Server.

Nimble ensures that snapshots are application-consistent for these volumes by using the vSphere APIs for backup and restore operations. Doing this also ensures that clones from these snapshots are consistent. The snapshot/replication schedule configured for a volume collection is controlled without extra requirements.

The sequence of synchronization steps is as follows:

- 1 Based on a schedule, NimbleOS connects to vCenter to determine the VMs present in the datastores on the Nimble LUNs in the volume collection.
- 2 vCenter Server queries ESXi to determine the list of VMs and returns the information to the Nimble array.
- 3 NimbleOS requests that vCenter Server take the snapshot of the VMs.
- 4 vCenter then communicates with the VMware VSS Services Support in VMware Tools to quiesce application writes to LUNs that correspond to volumes associated with the volume collection. Snapshot creation is then triggered, a VM application-consistent snapshot is created, and writes are unquiesced.
- 5 The array takes the snapshot of the volumes. The snapshot may be replicated to a remote array, depending on the schedule.
- 6 The VM snapshot is deleted.

Snapshot Exclusion and Inclusion Options for VMs and Datastores

By default, the VMware synchronized snapshots provided by NimbleOS include all the VMs and datastores in a volume collection. Starting with NimbleOS 4.2.0.0, you have the option of including or excluding specific VMs and datastores from the snapshot and its restore operation.

NimbleOS implements this option through the VMware Tags feature when you are running vCenter Server 6.0 or later. To use this option, you must first create a VMware tag category called **NimbleVMwareSyncSnaps** and then create two tags. The exclude tag is called **NimbleSnapExclude**, and the include tag is called **NimbleSnapInclude**. You can only apply these tags to VMware vSphere objects.

You have the following choices:

- **No tags.** If you do not create or assign any tags, the synchronized snapshot and its restore operations include all VMs and datastores. You do not have to take any action or apply any tags.
- **Exclude tag.** Any VM or datastore that has an Exclude tag associated with it is omitted from all synchronized snapshots and their restore operations.
- **Include tag.** Any VM or datastore that has an Include tag associated with it is always included in all synchronized snapshots and their restore operations.

You can have a mix of no tags, Exclude tags, and Include tags. You do not need to assign a tag to a VM or datastore unless you want to exclude it or explicitly include it.

For example, you might exclude a datastore, but include some of the VMs within it by associating them with the Include tag. When you associate a datastore with an Exclude tag, any VM within the datastore that does not have an Include tag is omitted from a snapshot operation or a restore operation for that snapshot. You can also associate a datastore with an Include tag. Then, any VM with an Exclude tag is omitted from a snapshot or restore operation and all other VMs, regardless of whether they have an Include tag, would be included.

Create a NimbleVMwareSyncSnaps Category

To use the VMware Tags feature to include or exclude a VM or datastore from a synchronized snapshot and its restore operation, you must set up a VMware category for the Exclude and Include tags. This category defines how you can use these tags.

The following steps explain how to create categories using the VMware vSphere Web Client.

Note You can also use other methods to create tag categories, including VMware vSphere PowerCLI cmdlets and the VMware vSphere APIs. See the VMware documentation for information on using those tools.

Before you begin

Make sure your environment includes the following:

- NimbleOS 4.2.0.0 or later
- vSphere Server 6.0 or later

Procedure

- 1 From the **Navigator** pane in the VMware vSphere Web Client, select **Tags & Custom Attributes**.
- 2 Select the **Tags** tab.
- 3 Select **Categories**.
- 4 Select the **Create** icon and perform the following tasks:
 - Create a category called **NimbleVMwareSyncSnaps** that has the **One Tag per object** attribute. This attribute ensures that only one tag from this category can be associated with a vSphere object at a time.
 - Under Associable Object Types, select **Datastore** and **Virtual Machine**. This selection ensures that these tags can be applied to only these objects.

Create Include and Exclude Tags

The Include and Exclude tags enable you to explicitly designate VMs and datastores to be excluded or included when VMware takes a synchronized snapshot or performs a restore operation for that snapshot.

Using these tags is optional.

Before you begin

Make sure your environment includes the following:

- NimbleOS 4.2.0.0 or later
- vSphere Server 6.0 or later
- A VMware tag category called **NimbleVMwareSyncSnaps**

Procedure

- 1 From the **Navigator** pane in the VMware vSphere Web Client, select **Tags & Custom Attributes**.
- 2 Select the **Tags** tab.
- 3 Select **Tag**.
- 4 Select the **Create** icon.
- 5 Create a tag called **NimbleSnapExclude** and associate it with the **NimbleVMwareSyncSnaps** category.
- 6 Create a tag called **NimbleSnapInclude** and associate it with the **NimbleVMwareSyncSnaps** category.

Assign Include and Exclude Tags to VMs and Datastores

You can assign **NimbleSnapExclude** and **NimbleSnapInclude** tags to VMs and datastores. The VMware tags feature allows you to explicitly designate VMs and datastores to be excluded or included when VMware takes a synchronized snapshot or performs a restore operation for that snapshot.

Using these tags is optional. You can use them with only some VMs and datastores while leaving the other VMs and datastores without tags. You can omit them completely. VMware synchronized snapshots always include VMs and datastores that have no tags.

Before you begin

Make sure your environment includes the following:

- NimbleOS 4.2.0.0 or later
- vSphere Server 6.0 or later
- A VMware tag category called **NimbleVMwareSyncSnaps**
- The VMware tags **NimbleSnapExclude** and **NimbleSnapInclude**

Procedure

- 1 From the **Navigator** pane in the VMware vSphere Web Client, select **Hosts and Clusters**.
- 2 Choose the vSphere object (VM or datastore) that you want to tag.
- 3 Select the **Manage** tab and click **Tags**.
- 4 Select the the **Assign Tag** icon.
- 5 Select the **NimbleSnapExclude** tag to exclude that VM or datastore from synchronized snapshots and their restore operations. Select the **NimbleSnapInclude** tag to include that object in those operations.
Note You cannot assign both tags to the same vSphere object.
- 6 Repeat these steps until you have assigned a tag to all the objects that you either want to exclude or to explicitly include. Any object that does not have a tag is automatically included in all synchronized snapshots and their restore operations.

Volume Collections and VMware Objects

The NimbleOS supports at most 16 vCenter synchronized snapshot schedules to run at a time. When 16 vCenter synchronized snapshot operations are in progress, any subsequent vCenter synchronized snapshot operation may result in only a crash-consistent snapshot being taken. An alert is issued indicating the failure to take a vCenter synchronized snapshot. We recommend that vCenter synchronized snapshot schedules be staggered such that at most 16 run in parallel. We also recommend that the snapshots be scheduled at a frequency of one hour or more.

You should schedule as few simultaneous vCenter synchronized snapshots as possible on the same ESXi cluster to reduce resource contention and obtain timely successful application-consistent snapshots.

When you select a volume collection that includes synchronization with VMware vCenter, you must define the vCenter host. This host is the central manager that manages all the virtual machines. The first time you use this option, you must provide the name of a user with Administrator access and that user's password to access the vCenter host.

After you complete the creation, return to the details page for the volume collection and click **Validate** to ensure that the username, password, and permissions are correct.

The following list includes the permissions that are checked on all the VMs in the datastores of the VolColl:

- VirtualMachine.State.CreateSnapshot
- VirtualMachine.State.RemoveSnapshot

The system displays either a success message or any issue that was found.

Volumes can be accessed from servers on virtual machines in the same way that physical servers access volumes. Synchronization is similar to any other synchronization-based schedules within the volume collection. When you apply a Protection Manager volume collection, you apply the snapshot schedule to all volumes assigned to that collection.

Because all volumes in the volume collection share the same schedules for snapshots and replication, stagger snapshot schedules so that not all the snapshot work is being done at the same time. For example, take hourly snapshots on the hour, and daily snapshots on the half-hour, and replicated snapshots every few hours on the fifteen-minute mark.

Common Tasks and Best Practices

This section provides instructions for common tasks and some best practices when integrating Nimble Storage and VMware.

VMware Partition Alignment

In virtualized file systems, multiple layers of storage are organized into blocks, which makes accessing the storage more efficient. The block size and the starting offset can differ at each layer. While block size may not be an issue across these storage layers, the starting offset is important.

For optimal performance, the starting offset of a file system should align with the start of a block in the next lower layer of storage. For example, an NTFS file system that resides on a LUN should have an offset that is divisible by the block size of the storage **group** presenting the LUN.

Misalignment of block boundaries at any one of these layers of storage can result in performance degradation.

Misalignment requires the **group** to read from or write to more blocks than necessary. VMFS partitions that are misaligned and must be manually aligned include certain VMFS partitions and certain Guest OS partitions.

There are no block alignment issues when using Nimble volumes as ESXi/VMware datastores if the datastore is created using the vCenter GUI with default settings. VMware aligns the datastore correctly.

Aligning Guest OS partitions

In the case of the Guest OS alignment on Windows, Windows Server 2008 and Vista partitions are aligned by default at 1024k. VMware does not recommend Windows boot disk alignment.

- **Windows Server 2003/2000/XP data disks**

Use `Diskpart` to create the disk partition. Be sure to specify a starting offset of 2,048 sectors (1 megabyte), which is the recommended offset and covers most stripe unit size scenarios. For details, see the Microsoft KB article at <http://support.microsoft.com/kb/929491>.

- **Windows Server 2008/Vista data disks** that are in-place upgrades from Windows server 2003/2000/XP

Use `Diskpart` to create the disk partition. Be sure to specify a starting offset of 2,048 sectors (1 megabyte), which is the recommended offset and covers most stripe unit size scenarios. For details, see the Microsoft KB article at <http://support.microsoft.com/kb/929491>.

- **Linux OS**

For Linux OS, use `fdisk` to align a partition manually:

- 1 Enter `fdisk -u /dev/sd <x>` where `<x>` is the device suffix.
- 2 Create the new partition by typing `n`.
- 3 Create a primary partition by typing `p`.
- 4 Choose partition 1 by typing `1`.
- 5 For the first sector, enter `2048`.
- 6 Use default value for the last sector.
- 7 Write the label and partition information to disk by typing `w`.

Register or Add VM to Inventory

You can register or add VMs to inventory using ESXi host or vCenter Server.

ESXi Host

Procedure

- 1 Use an SSH client to log in as root to the ESXi host.
- 2 Enter the following command:
vim-cmd solo/registervm /vmfs/volumes/<datastore name>/<VM directory>/<VM name>.vmx
 Make sure that the Virtual Machine name does not contain any Unicode characters.

vCenter Server

Procedure

- 1 Log into vSphere or the VMware client.
- 2 If connecting to vCenter Server, click on the desired host.
- 3 Click the **Configuration** tab, then click **Storage**.
- 4 Right-click the appropriate datastore and select **Browse Datastore**.
- 5 Navigate to the folder for the virtual machine, and locate the <virtual machine>.vmx file.
- 6 Right-click the .vmx file and click **Add to inventory**.
- 7 Complete the steps in the wizard to add the virtual machine to inventory.

Restore Entire Datastore to an Earlier Snapshot

Use this procedure:

- When the datastore only has one VM on it and you want to restore that VM to an earlier point in time without having to use a Nimble clone.
- When the datastore has multiple VMs on it and you want to restore *all* VMs to an earlier point in time without having to use a Nimble clone.

Note Be sure you want to restore ALL VMs.

Important When any volume is restored to an earlier snapshot, all I/O that was written since the last snapshot will be lost.

Procedure

- 1 If any VMs are running on the datastore that you are recovering, shut them down and remove them from inventory.
- 2 Remove all connections from all ESXi hosts to the volume. For each host:

ESXi 5.x only (prerequisite):

- a) Select the host in the vSphere Client, and go to the **Configuration / Storage** page.
- b) Right-click the datastore to be unmountefd, and select **Unmount**. Follow the onscreen prompts to unmount the datastore. The VMs must be powered off and removed from inventory.

ESX/ESXi 4.x, and ESXi 5.x (iSCSI):

- a) Select the host in the vSphere Client, and go to the **Configuration / Storage Adapters** page.
- b) Select the iSCSI Software Adapter and click the **Properties** link on the right-hand side of the screen.
- c) Go to the **Static Discovery** tab.
- d) Sort by the Target Name column, and expand the size of the window and column so you can see the entire names of all the volumes.
- e) Scroll down until you find the entries that match the Nimble volume name. Highlight all entries for the volume, and then click **Remove**. You can use Ctrl + click to highlight multiple entries.

- f) Answer **Yes** to confirm removal.
- g) When the removal completes, click **Close**.

Important You will be prompted to rescan, but answer **No**. **DO NOT RESCAN!** Rescanning picks up the connections you must removed.

- 3 Move to the Nimble GUI dashboard and select **Manage > Data Storage**.
- 4 Click on the appropriate volume. Go to the Data Protection tab to view the list of snapshots for that volume.
- 5 Check the snapshot containing the point in time you need to go back to. Click **Restore**.
- 6 Enable the box that confirms setting the volume offline. Click **OK**.
- 7 Re-establish all connections from all ESXi hosts to the volume. For each host:
 - a) Select the host in the vSphere Client, and go to the **Configuration / Storage Adapters** page.
 - b) Right-click on the iSCSI Software Adapter or Fibre Channel adapter, and select **Rescan**.
 - c) Move to the **Configuration / Storage** page and confirm that the datastore was rescanned and remounted.

When running ESXi 5.x, you may have to right click the datastore and select **Mount** to remount it.

- 8 For each VM in the datastore, navigate to its folder, and right-click the `.VMX` configuration file associated with it. Then select **Add To Inventory**.
Follow the onscreen prompts to add the VM back to inventory.
- 9 Power on each VM.
If the VM doesn't power on, look for a yellow exclamation point beside the VM name, right-click the VM, and select **Guest / Answer Question**. If asked whether you copied or moved the VM, answer **MOVED**.

Results

After the VMs have powered on and are running, the restore operation is complete.

Recover a VMware Volume from a Cloned Snapshot

Restoring a VMFS-consistent volume from a cloned snapshot prevents the original volume from getting overwritten with data from a previous snapshot. A clone is actually a new volume. Use this method of restoration if you have more than one VM per volume.

The process of recovering data from a VMware snapshot is slightly different than restoring a non-VMFS-consistent snapshot. To restore a VMware volume using the NimbleOS GUI:

Procedure

- 1 From the main menu, select **Manage > Data Storage** to access the volume details screen. Select the snapshot from which the volume will be recovered.
- 2 Clone the volume as described in the *GUI Administration Guide*.
The cloned volume is automatically set to online and should contain the initiator group assigned to the original volume.
- 3 In vCenter, select the Storage Adapter for iSCSI or Fibre Channel and click **rescan all**.
You should see the new cloned volume in the devices section.
- 4 While still in vCenter, select the Storage section and choose **Add Storage**.
Your newly cloned volume should appear in the list of storage available to add.
- 5 Select the new clone and click **Next**.
You are prompted to keep or assign a new signature.
- 6 Click **Assign a New Signature**.

Note Nimble recommends that you always re-signature at this point. Your cloned volume now appears as a datastore.

- 7 Remove your original VM from inventory.
- 8 Browse to the new cloned volume datastore for your VM and add the recovered VM to inventory.
- 9 While still in vCenter, right click on the VM and choose **Snapshot > Snapshot manager**. There should be a single snapshot in the list. Select **Revert to snapshot**.
You will only see a VMware snapshot if the volume was in a volume collection that was taking vCenter Synchronized snapshots. Manual snapshots or non-synchronized snapshots will not have a VMware snapshot.
- 10 To move the recovered VM to its original volume, right click on the VM, and select the Migrate option.

Change the VMware vCenter Access Information

If the IP address or host name of your VMware vCenter Server changes, change the access information on any volume collection that uses the selected synchronization method to reflect the new configuration.

Change Access Information Using the Editing Wizard

Procedure

- 1 From the NimbleOS main menu, select **Manage > Data Protection**.
- 2 Check the volume collection that uses the synchronization option you want to change to show its details.
- 3 Click **Edit** (the pencil icon).
The editing wizard opens.
- 4 Make any necessary changes.
- 5 Click **Save**.
- 6 Repeat this procedure for each volume collection using synchronization.

Change Access Information Using the CLI

To change VMware vCenter access information using the NimbleOS CLI:

Procedure

Edit the volume collection information.

```
volvoll --edit collection_name [--newname new_collection_name] [--description description] --app_sync
[none | vss | vmware] --app_server host-name
```

Example

```
volcoll --edit collection33 --app_sync vmware --app_server 10.15.133.70
```

VMware iSCSI Best Practices

Here are some iSCSI-specific best practices when using VMware and the Nimble array. Adhering to these practices will help ensure that iSCSI connectivity is maximized and that communication between the network components is optimized for best performance.

- There must be a one-to-one mapping between vmkernel (vmk) ports and physical (vmnic) NIC ports.
- If you are using multiple VLANs for iSCSI traffic, use separate vSwitches for each VLAN.
- If you are using a single vSwitch, disable NIC Teaming.
- Use the Nimble Storage custom round robin policy and IOPS adjustment for optimal performance.
- Ensure all vmkernel (vmk) ports are only bound to the software iSCSI initiator when on a single iSCSI network, and not when multiple iSCSI networks are used.
- Ensure all VM guest machines using direct attached or Raw Device Mapped (RDM) volumes are connecting to the array over additional interfaces, not those with bound kernel ports to the iSCSI adapter.
- Use Jumbo Frames (MTU 9000 or larger) for both the physical switches and the Nimble array.

For more information, see [Manual VMware iSCSI configuration](#) on page 9 in this document and also see the [VMware iSCSI SAN Configuration Guide](#). Also see the switch manufacturer's documentation.

Important

iSCSI Target Limits

The maximum number of iSCSI static (manually assigned IP addresses) or dynamic (IP addresses assigned to discovered targets) allowed per adapter port is between 62 and 128, depending on the initiator model.

The sum of all iSCSI software targets, either manually assigned or dynamically discovered, cannot exceed 256.

For more information, refer to the *Configuration Maximums – VSphere 6.0* and *Configuration Maximums – VSphere 6.5* documents, available at

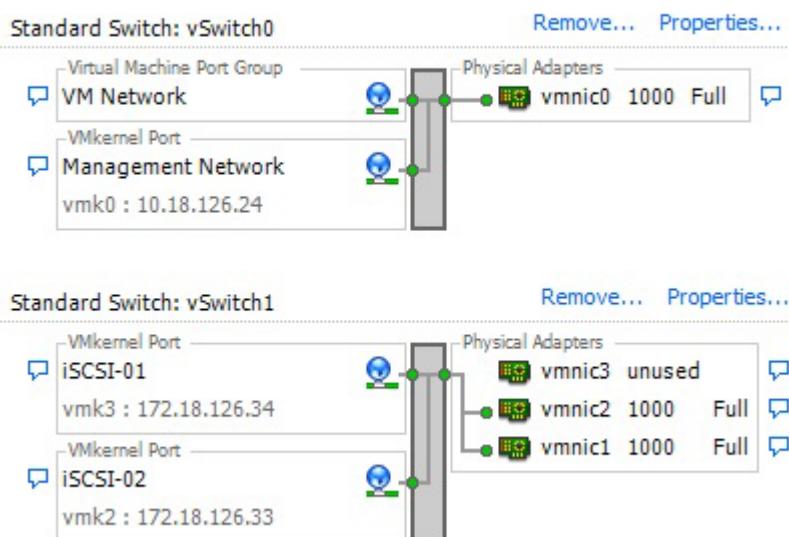
<https://www.vmware.com/pdf/vsphere6/60/vsphere-60-configuration-maximums.pdf> and

<https://www.vmware.com/pdf/vsphere6/65/vsphere-65-configuration-maximums.pdf>, respectively.

VM Guest Machines

Below are two VMkernel ports corresponding to two physical adapters on the ESXi server. These two VMkernel ports and vmnics represent the iSCSI connections from an individual ESXi server to the Nimble array.

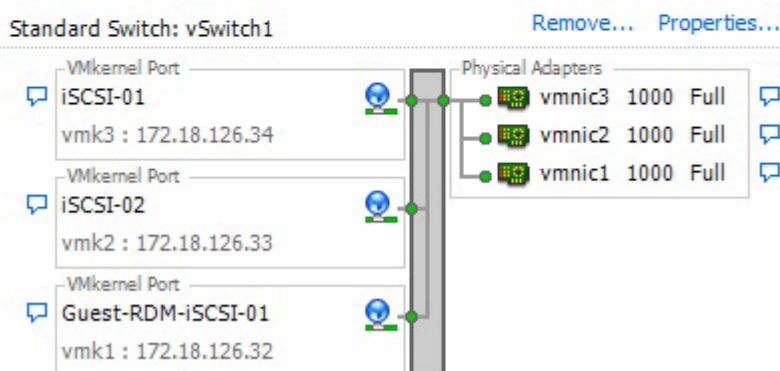
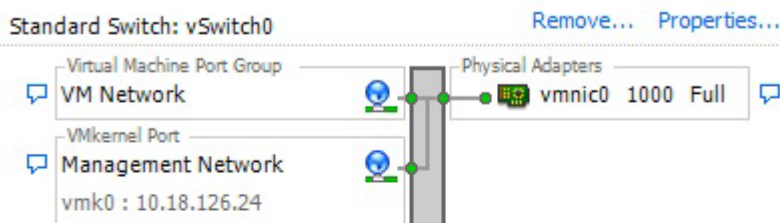
Networking



In certain configurations, some VMguest hosts can be configured to interact directly with the Nimble array through iSCSI connections from the VMguest OS or through RDM. When connecting from the VMguest OS to the array in this manner, add an additional vmnic to each vswitch that will be conducting iSCSI traffic.

The creation of an additional iSCSI kernel port using only vmnic03 will guarantee that the utilization of this network adapter is solely used for VMguest, which requires direct access to the Nimble array through RDM or direct iSCSI attachment. In this example, we have named the additional iSCSI VMkernel port "Guest-RDM-iSCSI-01".

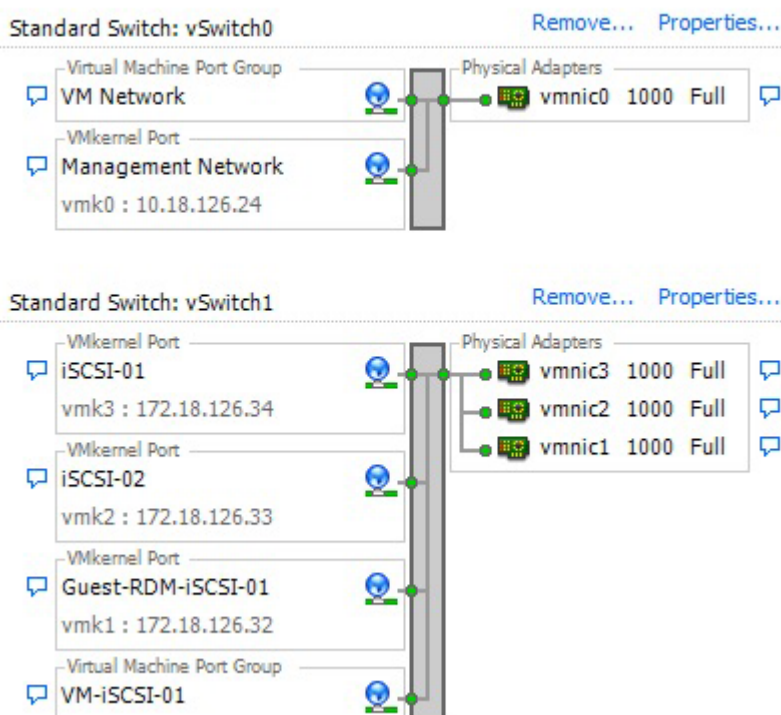
Networking



Edit the newly created iSCSI VMkernel port to modify the failover override in the same manner as the previous VMkernel ports for ESXi server to Nimble array iSCSI traffic.

Create a virtual machine group assigned to use the corresponding iSCSI VMkernel port with its assigned vmnic.

Networking



Edit the new virtual machine group named "VM-iSCSI-01" to modify the failover override so it will use only the vmnic assigned to the designated iSCSI VMkernel port, which is labeled "Guest-RDM-iSCSI-01" in the diagram.

Multiple iSCSI kernel ports can be assigned to a single virtual machine group, as needed for iSCSI path redundancy. To add additional paths to the virtual machine group, additional adapters must be available and VMkernel iSCSI ports must be created for those adapters. Then the vmnic must be assigned to the virtual machine group. This is accomplished by editing the virtual machine group and adding the corresponding vmnic to the "active" section of under the NIC Teaming tab.

Managing Target Subnets

Each NIC on a VMware host attempts to connect to each of the NICs on the Nimble array, over all available subnets. Many of those paths are invalid, resulting in a number of dead paths, which are eventually removed. But before removal, the dead paths count toward the maximum of 1024 paths supported by the VMware host. This situation results in long periods of time required for boot, scan, and rescan.

To shorten the boot, scan, and rescan time periods, use iSCSI initiator groups to limit the number of connections between the VMware host and the array to a specific subnet. Using iSCSI initiator groups means that only the NICs on associated subnets are visible to the host. As a result, the host does not attempt to make all theoretically possible connections.

An iSCSI initiator group consists of one or more subnets and one or more host initiators. You can create an iSCSI initiator group using the NimbleOS GUI or CLI. After you create your iSCSI initiator groups, assign your volumes to them.

See [iSCSI Initiator Groups](#) on page 136.

Rapid Cloning of a VM Using Nimble's LUN Cloning

The basic steps for rapid cloning are cloning a volume/LUN (datastore) using Nimble's cloning on the **array**, and then making vCenter or the ESXi host aware of the new datastore and VM.

These instructions assume usage of vSphere connected to a vCenter server or connected directly to an ESXi host. They also assume that the iSCSI adapter on the ESXi host is already configured with a dynamic discovery address.

Note Before beginning, make sure that the advanced setting in ESXi that automatically re-signatures snapshots/clones (LVM/EnableResignature) is turned OFF.

This workflow consists of the following major steps:

Procedure

- 1 [Prepare a VM/LUN as a template.](#)
- 2 [Perform steps on the guest OS](#) (such as sysprep for Windows).
- 3 [Create a VM clone.](#)

Prepare a VM or a LUN as a Template

Use this procedure to perform rapid cloning on your Nimble array.

Procedure

- 1 Create a single volume that is large enough to hold the VM on the Nimble array.
 - a) In the Nimble GUI, select **Manage > Data Storage**.
 - b) Click **Add**.
 - c) Follow the steps in the wizard.
- 2 Log into vSphere and create a VMFS datastore on the volume or LUN:
 - a) In the vSphere *Hosts and Clusters* view, select the host.
 - b) Tab to *Configuration* and select **Storage Adapters**.
 - c) Select the iSCSI or Fibre Channel adapter and in the upper right click **Rescan**. Depending on the connected SANs, this may take a few minutes to complete.
 - d) After the rescan is complete, click the **Storage** link and in the upper right click **Add Storage....**
 - e) Select **Disk/LUN** then click **Next**.
 - f) Select the newly created volume. You might need to expand the **Path ID** column to see the full path containing the actual volume name for the iSCSI target.
 - g) Accept all the default options to format it as a VMFS datastore.
The volume should now appear in the datastore list.
- 3 On the host and using the new datastore, create a new VM or migrate or clone an existing one.
- 4 Power off the VM.

What to do next

Complete the steps in the [Perform Steps on the Guest OS](#) on page 57 section.

Perform Steps on the Guest OS

After preparing a VM/LUN as a template, complete these steps to enable rapid cloning on your Nimble array.

Before you begin

Prepare a VM/LUN as a template.

Procedure

- 1 Set the network interfaces to **DHCP**.
- 2 If desired, create a VMware Guest Customization Specification, accessible through the vCenter **Edit > Customization Specifications...** menu.

Note Do not set the VM to **template**, which would cause clones to be templates.

What to do next

Complete the steps in the [Create a VM Clone](#) on page 58 section.

Create a VM Clone**Important**

Create one clone at a time. Do not create multiple clones, as ESXi can resignature one clone at a time.

Before you begin

Complete the steps on the guest OS to enable rapid cloning.

Procedure

- 1 Clone the volume/LUN that holds the VM template:
 - a) Log into the Nimble array. From the GUI, select the volume to clone, then click **Take Snapshot**.
 - b) If desired, create a VMware Guest Customization Specification, accessible through the vCenter **Edit > Customization Specifications...** menu.
 - c) Move to the *Snapshots* tab on the volume, select the snapshot, and click **Clone**.
- 2 In the vSphere GUI, select the host on which you want the new VM.
- 3 On the host's *Configuration* tab:
 - a) Select **Storage Adapters** and then the iSCSI or Fibre Channel adapter.
 - b) In the upper right, click **Rescan**.
Depending on the connected SANs, this may take several minutes to complete.
 - c) After the rescan completes, move to the *Storage* link and click **Add Storage...**
 - d) Select **Disk/LUN**, then click **Next**.
 - e) Select the newly cloned volume. You might need to expand the "Path ID" column to see the full path containing the actual volume name.
 - f) When you are presented with the VMFS mount options, select **Assign a new signature**.
 - g) Click **Next** and **Finish** to move through the remaining creation steps.

Note Do not set the VM to **template**. That would cause the clones to be templates.

The new volume appears in the datastore listing as `snap-<randomhex>-volumename`, where the last part of the name is the template's volume name, not the clone volume name.

- 4 To rename the volume, right-click and select **Rename**. Enter the new name.
- 5 Right-click the new datastore and select **Browse this datastore**.
- 6 Highlight the VM folder and select the `.vmx` file (or `.vmxt` if the volume is a VM template).
- 7 Right-click and select **Add to inventory**. When prompted for the source of the VM, confirm that it was **copied**.
- 8 Provide a name for the VM and any other requested information, such as in which host, cluster, and resource pool to put the VM.
- 9 Power on the VM.
- 10 Repeat these steps for all additional clones.

Using VMware RDM disks

If you want to use shared RDMs, you must make sure the guest operating system is clustered. For more information, see the VMware Knowledge Base article [Sharing an RDM virtual disk between multiple virtual machines \(1002782\)](#).

Important

An I/O error can occur on VMs with RDM devices when you are running vSphere versions 5.1 or 6.0. See your VMware documentation for more information.

If you encounter this problem, configure the virtual machine with the RDM to ignore the SCSI CACHE inquiry file by adding the following parameter to the .vmx file:

scsix:y.ignoreDeviceInquiryCache = "true"

Where x is the SCSI controller number and y is the SCSI target number of the RDM.

To add an RDM disk to a VM, complete the following steps:

Procedure

- 1 Attach the volume to be used as the RDM to the ESXi host. Do not add a datastore.
- 2 Add the ESXi initiator or WWPN to the initiator group for the RDM volume.
- 3 Edit the settings on the VM that will use the RDM volume, adding the disk (RDM) and select the Nimble volume.

Results

After adding the RDM disk to the VM, it appears as a regular disk in the guest OS.

Nimble LUNs in the Device List

Even though the vCenter iSCSI discovery was successful, you might find that none of the Nimble volumes appear in the list of devices. To verify this on an iSCSI adapter:

Procedure

- 1 Ensure that the dynamic discovery IP address has been configured.
- 2 Select **Storage Adapters** and then the iSCSI adapter. Click **rescan**.
- 3 After the rescan completes, move to the Storage link and click **Add Storage...**

Results

If you still don't see any Nimble LUNs in the **Select Disk/LUN** list, it is possible that the ESXi host is not in the volume access control list. Verify that the volume ACL is correctly assigned to the ESXi host. If the volume is expected to be accessed by multiple ESXi hosts, enable the volume option to **Allow multiple initiator access**.

Locate vCenter logs

Procedure

- 1 In Windows, vCenter logs are usually located in C:\ProgramData\VMware\VMware VirtualCenter\Logs. Logs are named vxpd-*nnnn*.log, where *nnnn* is an incrementing number.
- 2 If you cannot find the logs, open Windows Explorer (not Internet Explorer) and choose **Tools > Folder Options**. Enable *Show hidden files and folders*.

Unresponsive vCenter

Symptoms of an unresponsive vCenter server include the server stopping when a client first connects, the event viewer showing a `vxpd.exe` problem, and the `vxpd` log shows "Win32 Stack Overflow" error for the same time as the event seen in the event viewer.

Procedure

- 1 `vxpd.log` is in `C:\ProgramData\VMware\VMware VirtualCenter\Logs`. It is frequently rotated, use the latest one.
- 2 Check for entries on the same time as the Windows event.
- 3 Change log level to **trivial**.

Results

The most common cause seen in testing has been that a VM may have a VMDK that is split up into too many files, despite showing no snapshots for it in vSphere.

VAAI Integration

The Nimble array lets you take advantage of VMware's vStorage APIs for Array Integration (VAAI). It reduces the time that it takes when you provision new VMs. Therefore you can easily support large-scale VMware or virtual desktop (VDI) deployments. This feature is automatically installed.

What is VAAI?

vStorage APIs for Array Integration (VAAI) is a set of features that provide hardware acceleration. VAAI enables the ESXi host to offload VM and storage management operations to the Nimble array. As a result, ESXi host performs these operations faster while consuming fewer resources.

The following VAAI primitives are supported starting with NimbleOS 1.4 and later:

- Atomic Test and Set Locking (ATS) – The ATS feature is used for file locking to control access to datastores by multiple ESXi hosts.
- Zero Blocks/Write Same – This feature is used to zero-out large numbers of blocks on VMDKs (both thick and thin) at the same time.
- Block Delete/SCSI UNMAP – The UNMAP feature is designed to efficiently reclaim any deleted space to meet continuing storage needs.

Important On ESXi 5.0u1 and later servers, the VAAI UNMAP primitive is disabled by default. You must enable it manually. See the ESXi server documentation.

- Thin Provisioning Stun – The Thin Provisioning Stun primitive provides a mechanism by which the array is able to return warnings to the hypervisor when space thresholds are exceeded.

See [VMware KB article 1021976](#) for details.

The following VAAI primitives are supported starting with NimbleOS 3 and later:

- Extended Copy (XCOPY) – The Extended Copy primitive requests the array to perform a full copy of blocks and is used primarily in clone and migration operations.

Enable the VMware VAAI Provider to use Nimble Volumes

When you use NimbleOS with VMware vCenter servers, you can take advantage of the VAAI "write same" (also called block zeroing) primitive provided by VMware. Everything necessary to enable the VAAI write-same feature is included with the NimbleOS. No installation is required.

If you are using ESXi 5.0 or later, VAAI is enabled by default. After triggering a write-same operation, VAAI shows status as *supported*; for example, the "Zero Status" line appears as "supported" in the following output:

```
~ # esxcli storage core device vaai status get --device
eui.ac839379d23f153f6c9ce90069fd976d
eui.ac839379d23f153f6c9ce90069fd976d
VAAI Plugin Name:
ATS Status: unsupported
Clone Status: unsupported
Zero Status: supported
Delete Status: unsupported
```

If you are using ESX/ESXi 4.x, you must instruct VMware that the volumes in your Nimble group support the primitive by enabling the procedure below. This procedure uses the native `vmw_vaaip_t10` plugin.

Note Commands are case sensitive.

Procedure

- 1 Log into the ESX/ESXi 4.x host server.
- 2 At the command prompt, enter these commands:
 - a) **esxcli corestorage claimrule add --claimrule-class VAAI --plugin VMW_VAAIP_T10 --type vendor --vendor Nimble --autoassign**
 - b) **esxcli corestorage claimrule add --claimrule-class Filter --plugin VAAI_FILTER --type vendor --vendor Nimble --autoassign**
 - c) **esxcli corestorage claimrule load --claimrule-class VAAI**
 - d) **esxcli corestorage claimrule load --claimrule-class Filter**
 - e) **esxcli corestorage claimrule run --claimrule-class Filter**

- 3 Verify that the values for the claimrule commands were added correctly.

esxcli corestorage claimrule list --claimrule-class VAAI

- 4 Verify that the VMware VAAI T10 provider has claimed the Nimble volumes.

esxcli vaai device list

The device shows a message similar to:

```
eui.70895ce68ed286546c9ce900e77326f6
  Device Display Name: Nimble iSCSI Disk
(eui.70895ce68ed286546c9ce900e77326f6)
  VAAI Plugin Name: VMW_VAAIP_T10
```

Note Known issues in which block zeroing does not work optimally:

- If you are using existing VMFS v3.33 datastores (created with ESX 4.0) on VAAI-enabled hosts, VAAI block zeroing does not improve performance. This is not an issue for newly created datastores on VMFS v3.46. Datastores cannot be upgraded to a newer VMFS version.

See [this KB article](#) for details.

- If you used the vSphere UI to create a VM or VMDK as *thick*, it only shows speed improvement when you use the *-D eagerzeroedthick* option on the ESX CLI.
- When you extend a VMDK, even with the *-D eagerzeroedthick* option enabled, using block zeroing does not speed up performance.

The Nimble vCenter Plugin

Nimble Storage provides a plugin that works specifically with vCenter to manage datastores residing on Nimble arrays. You can use either the desktop vCenter plugin, or the web-based vCenter plugin. Both provide the same functionality, with slight variances in the user views, and minor enhancements. For more information, or to start using the web client, see [The Nimble vCenter Web Client Plugin](#) on page 78.

The Nimble vCenter plugins allow you to do the following:

- Create, clone, grow, and edit datastores
- Take, clone, and delete snapshots
- Add Nimble-specific capabilities to vCenter server which can be used to create vCenter roles
- Edit protection schedules

Important For the vCenter plugin, you must be running ESXi 5.5 update 1 or later.

Note If the array is in a VMware environment, best practice indicates that you have ACLs (iSCSI initiator group and/or CHAP username) on all volumes.

The following privileges are required for using the vCenter plugin.

- Datastore.AllocateSpace
- Datastore.Config
- Datastore.Delete
- Datastore.Move
- Datastore.Rename
- Extension.Register
- Extension.Unregister
- Extension.Update
- Global.CancelTask
- Host.Config.AdvancedConfig
- Host.Config.NetService
- Host.Config.Settings
- Host.Config.Storage
- StoragePod.Config
- System.Anonymous
- System.Read
- System.View
- Task.Create
- Task.Update

Register the vCenter Plugin Using the NimbleOS CLI

The plugin is part of the NimbleOS. To take advantage of the plugin, you must first register it with a vCenter Server.

You can register multiple plugins on the Nimble array. Each array that registers the plugin adds a tab to the vSphere client. The tab name for the datastore page is "datacenter page-Nimble-<groupname>".

Before you begin

Important The vCenter plugin is supported on ESXi 5.5 update 1 and later.

Note

The plugin is not supported for:

- Multiple datastores located on one LUN.
- One datastore spanning multiple LUNs.
- LUNs located on a storage device not made by Nimble.

Use a vCenter account that has sufficient privileges to install a plugin (usually a user assigned to the Administrator role). You need to know the vCenter hostname or IP address.

Procedure

- 1 Log into your Nimble array using the NimbleOS CLI.

See [Log in to the NimbleOS CLI](#) on page 133.

- 2 At the command prompt, type:

```
vmwplugin --register --username <username> --password <password> --server  
<server_hostname-address> --subnet_label <subnet_label>
```

Depending on which vCenter client plugin you are registering, add the following command option:

- **--client thick** (for desktop)
- **--client web** (for web client)

- 3 Restart the vSphere client.

Results

If the registration was successful:

- When you click a datacenter, the datacenter includes a Nimble array <group-name> tab.
- When you click a specific datastore, the datastore includes a Nimble Datastore tab. The tab name for datastore page is the same as the datacenter page – “Nimble <group-name>”

Register the vCenter Plugin Using the NimbleOS GUI

Registering a vCenter enables Nimble Storage to collect VMware configuration data and per-VM monitoring statistics. Analytics collected provide insights into performance and usage that can be seen via InfoSight.

Procedure

- 1 Go to **Administration > VMware Integration**.
- 2 Click **Add Another vCenter** at the bottom of the page.
- 3 On the Register a vCenter page, complete the required information.
- 4 Click **Save**.

View a List of Registered Plugins

You can view a list of all registered plugins.

Procedure

- 1 Log into the NimbleOS CLI.

See [Log in to the NimbleOS CLI](#) on page 133.

- 2 At the command prompt, type:

```
vmwplugin --list --username <username> --password <password> --server  
<server_hostname-address> --port port_number <port number>
```


Note If no port number is specified, port 443 is selected by default.

A list of registered plugins displays.

Create Roles (Role-Based Permissions)

Role-based permissions protect access to Nimble-based datastores and actions taken on them.

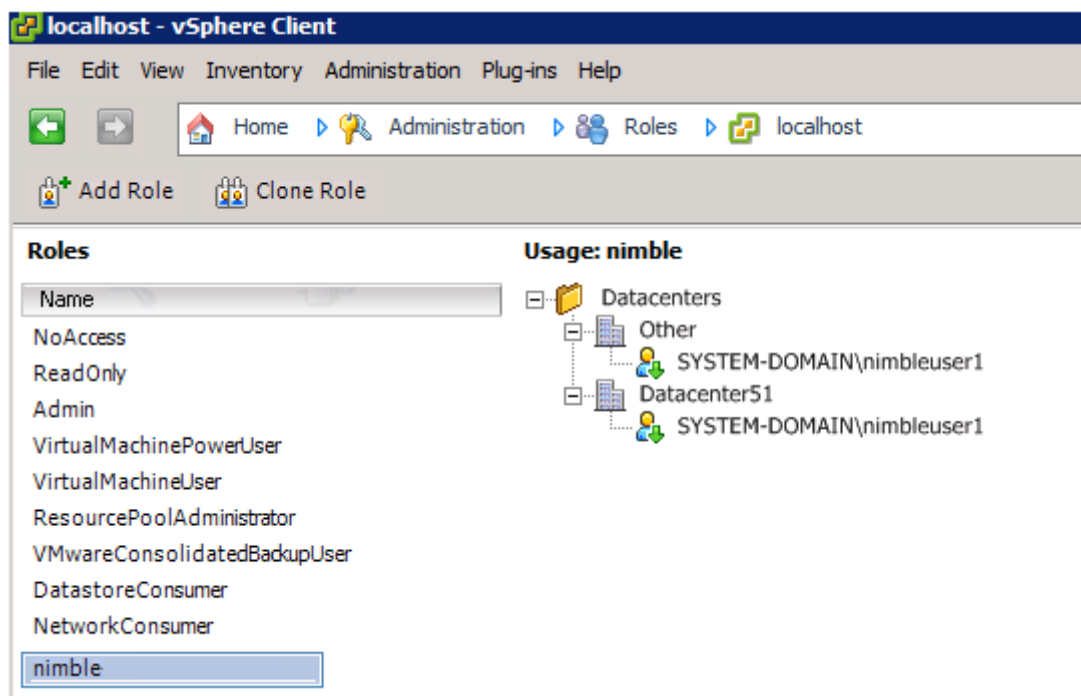
Actions taken on Nimble-based datastores are based on roles with Nimble-specific permissions that allow or disallow features. All user roles must have a minimum of permissions listed under the Nimble Storage, Inc. permissions dialog box. There is no default role.

To add a role:

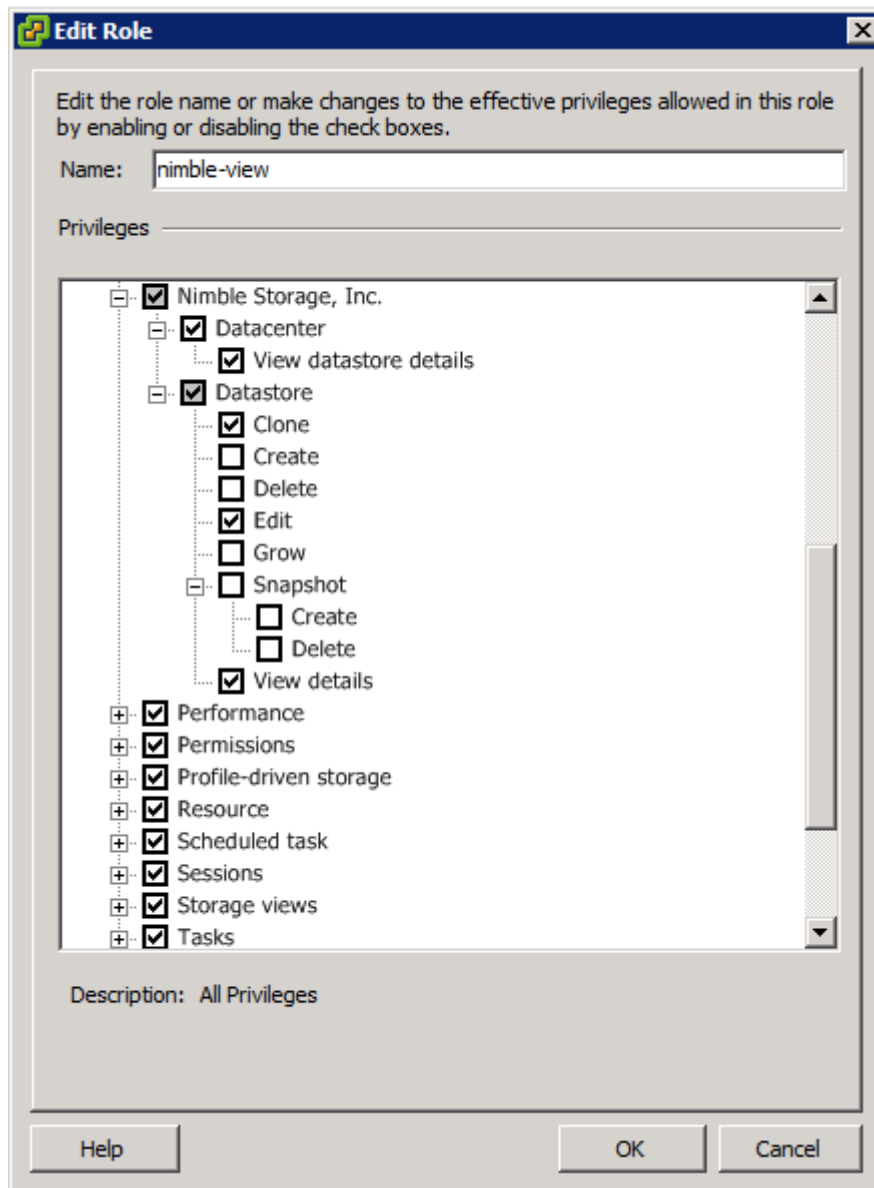
Procedure

- 1 Log into the vCenter client.
- 2 Select **Home > Administration > Roles**.
- 3 From the Roles dialog box, click **Add Role**.
- 4 Enter a name for the role and an optional description.

The following shows an example of the newly added role *nimble*:



- 5 Check the boxes beside the permissions enabled for this role.
Select all permissions to be allowed for this role.



Note

- Permissions under Nimble Storage, Inc. are specific to datastores on Nimble Storage arrays.
- Permissions must be explicitly granted for actions such as creating, cloning, deleting, and all other activities.
- If a role does not include a particular permission, the users assigned to that role do not see the options based on that permission.
- Each role must have Nimble Storage, Inc. permission and Datacenter > View datastore details permission.
- To view the plugin in a datastore context, you must enable:
 - Nimble Storage, Inc.,
 - Datastore, and
 - View details

When disabled, the datastore is not visible nor editable. No action such as creating, cloning, or any other activity can be taken on the datastore.

- 6 Click **OK**.

Create a New Datastore

The Nimble vCenter plugin enables you to create VMware datastores that are mapped to volumes on the Nimble array.

Procedure

- 1 Log in to the vSphere client connected to vCenter.
- 2 Select the datacenter under which you want to create the datastore.
- 3 Navigate to the tab for the vCenter plugin with name *Nimble <group-name>*.
- 4 Click the Add icon (+) to launch the new datastore wizard.
- 5 Enter a datastore name, an optional description, and the hosts to which you want to allow access to the new datastore.

Hosts can be inside or outside of a cluster, but they must be in the same data center. If a host is within a cluster you must select the cluster, meaning that all hosts in the cluster are granted access. Offline hosts cannot be selected.

Note If the group supports Fibre Channel, only Fibre Channel hosts are listed.

New Datastore

1 General

2 Size

3 Protection

4 Schedules

5 Summary

Datastore Name: sample

Description: sample datastore

Select Hosts:

Filter by name of host

- ▼ vCenter
 - ▼ Datacenter51
 - ▼ cluster41
 - ☐ 10.18.208.44 (v.4.1.0)
 - ☐ 10.18.208.11 (v.4.1.0)
 - ▼ ☒ cluster51
 - ☒ 10.18.208.78 (v.5.1.0)
 - ☒ 10.18.208.94 (v.5.1.0)
 - ☐ 10.18.208.64 (v.5.0.0)
 - ▼ Other

Back Next Finish | Cancel

When Data Encryption is enabled on the Group or Volume, the option appears at the bottom of the General screen:

If data encryption is enabled on the Group, only the Administrator can disable it from the array, or choose to encrypt the volume. When encryption is enabled on the Volume, users with permissions can choose to enable or disable the option during datastore creation.

- Enter the desired size and space use information into the appropriate fields, then click **Next**. The graphic information on the right of the page is provided as a visual cue.

Note As shown in the images above, if the pool selected is capable of deduplication, the checkbox is enabled. If the pool is not capable of deduplication, the checkbox is visible but disabled. When deduplication is checked, the datastore and snapshot reserve space is set to 0.

If all hosts are ESX 5.0 or later, VMFS 5 is used and the block size is set at 1 MB and cannot be changed. Older ESX versions use VMFS 3 and require you to set the appropriate block size.

DATA

Datastore Size: VMFS Block Size:

Storage Pool:

- 7 Define the protection options and synchronization options, then click **Next**.

Note CHAP users are configured both on the ESX hosts and the array.

If you enable synchronized snapshots, you must include the vCenter host and log in information. See the *Nimble Storage Administration Guide* for protection definitions.

General

1 General

2 Size

3 Protection

4 Schedules

5 Summary

Volume collections are used to protect datastores using similar schedules. It's recommended that you choose an existing volume collection or create a new volume collection.

☐ None

☒ Create new Volume Collection:

☐ Join existing Volume Collection:

☐ Protect as Standalone Volume

Application-consistent snapshots can be taken by enabling synchronization. To enable synchronization, please provide your vCenter credentials below.

☒ Configure synchronized snapshots

vCenter Host:

User Name:

Password:

- 8 Create or choose the schedules.

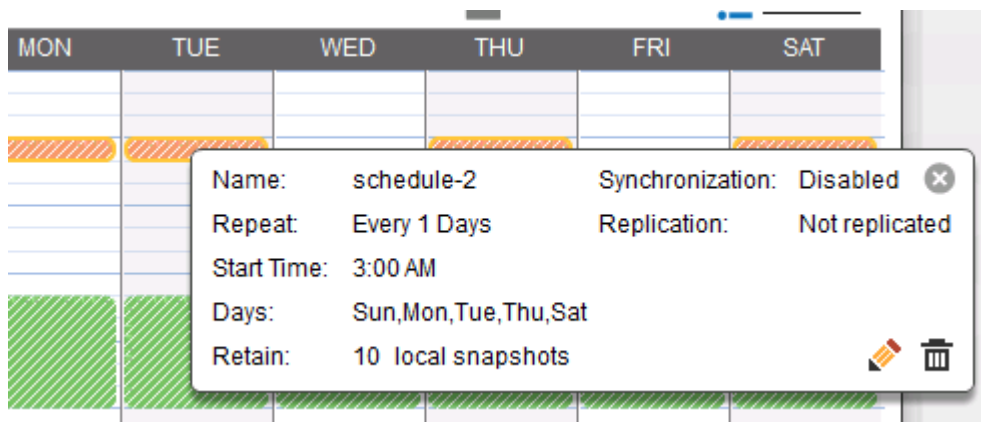
The screenshot displays the 'Protection' console with the 'Schedules' tab selected. The 'Add a Schedule' button is highlighted with a red circle and a red arrow pointing to the 'Add a Schedule' dialog box. The dialog box contains the following fields:

- Name:** schedule-1
- Snapshots:** Repeat: 1, Hours, Start: 10:00 AM, End: 03:00 PM, Days: Every day, Retain: 10 local snapshots
- Synchronization:** Enabled (radio button), Disabled (radio button)
- Replication:** Replicate to: None

The background shows a calendar grid with columns for days of the week (SUN, MON, TUE, WED, THU, FRI, SAT) and rows for times of day (12 AM, 3 AM, 6 AM, 9 AM, 12 PM, 3 PM, 6 PM, 9 PM). The 'Add a Schedule' button is located at the top left of the calendar grid.

Click **Add a Schedule** to add a new schedule to the datastore protection. Use the calendar to create schedules, enable synchronization, and set replication levels. Schedule types are color-coded for easy recognition, and the legend appears at the bottom of the page. Create and add as many schedules as needed.

In the list view, hover over a schedule to see a summary of the schedule, or click the schedule to see details.



9 Click **Next**.

10 View the settings summary and click **Finish**.


A new task appears in the task list to show you that the datastore is being created. After completion, the new datastore appears in the datastore list for the datacenter.

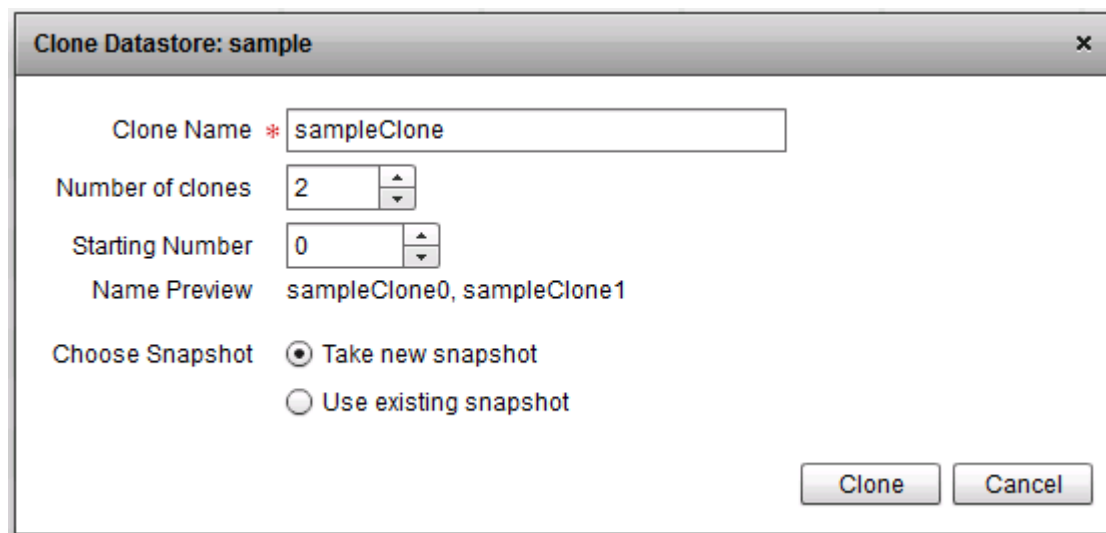
Clone a Datastore

The Nimble vCenter plugin enables you to clone VMware datastores that reside on a Nimble array. Clones are created from snapshots.

Procedure

1 Start the vSphere client connected to vCenter and navigate to the Datastores list view.

2 Click the Clone icon (), or from the list view, select the datastore, right-click, and select **Clone**. The snapshot to be cloned is shown at the top of the dialog box. Make sure that the correct snapshot is selected.



3 Enter a name for the clone.

4 Select the number of clones to create.

5 For multiple clones, enter the **Starting number** for clones.

The Starting Number selector only appears when the number of clones is greater than one. When creating multiple clones, all clones created at this time have the same name with a number appended, for example MyClone1, MyClone2, MyClone3, and so on. Clone name/numbers will be incremented from this number. For example, if you create five clones and set the starting number to 7, the clones will be named MyClone7, MyClone8, MyClone9, and so on.

- 6 Choose to use an existing snapshot or take a new one. If you choose to use an existing snapshot, the system presents a list of snapshots for selection.
- 7 Click **Clone**.

The Active Tasks list shows an activity titled Clone Nimble Datastore and all of the subtasks.

Results

After the datastore is successfully cloned, all hosts that had mounted the original datastore also show the cloned datastore.


Grow a Datastore

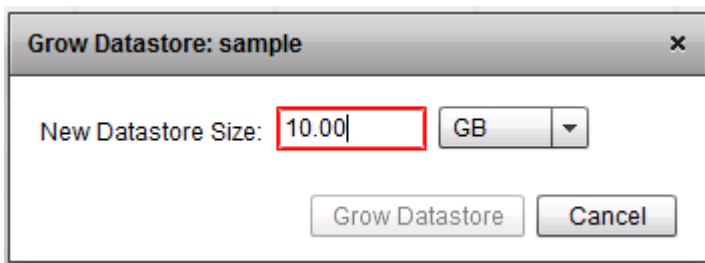
This procedure enables you to grow or resize a datastore.

If you have the correct permissions to do so, you can increase the size of a Nimble datastore.

Important To avoid selecting the wrong device during a grow operation, we recommend using the Nimble vCenter Plugin to grow any Nimble datastore.

Procedure

- 1 Start the vSphere client connected to vCenter.
- 2 Select the datastore you want to grow.
- 3 Click the Grow  icon.
The current datastore size displays. Type the new size and select the unit type.
- 4 Increase the size of the datastore to activate the **Grow Datastore** button.
The minimum growth size is 1GB. The GUI does not allow you to shrink a datastore.



- 5 Click **Grow Datastore**.
The Active/Recent Tasks area shows the in-progress growth as a task and any subtasks.

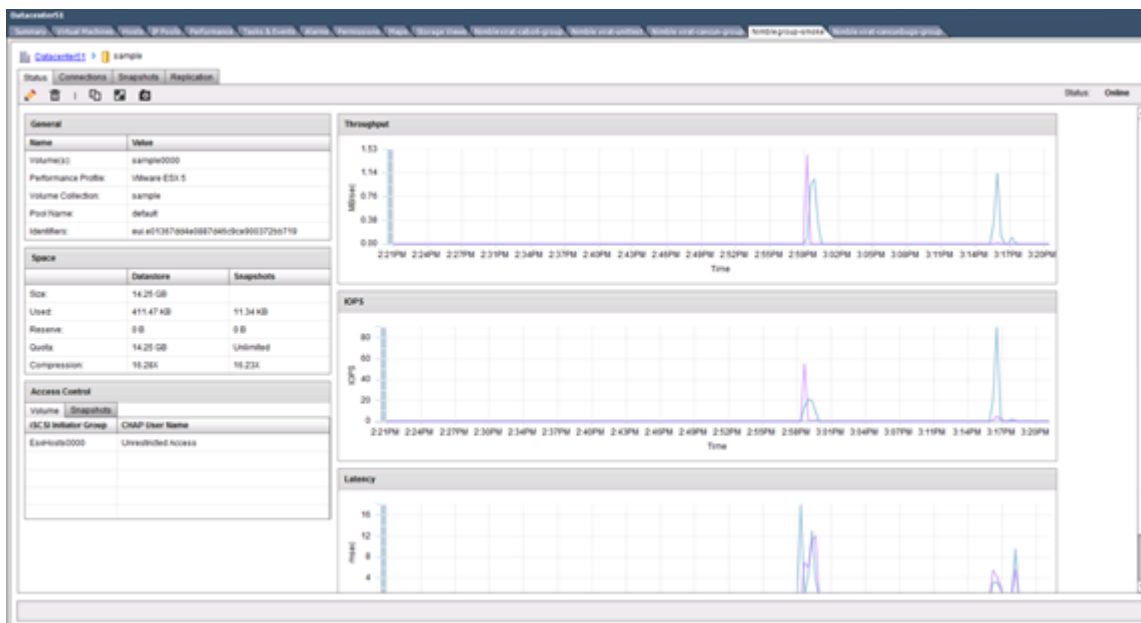
Recent Tasks		
Name	Target	Status
Rescan VMFS	10.18.208.78	Completed
Rescan VMFS	10.18.208.78	Completed
Rescan VMFS	10.18.208.94	Completed
Rescan HBA	10.18.208.78	Completed
Rescan HBA	10.18.208.94	Completed
Grow Nimble datastore	sample	Completed
Expand VMFS datastore	10.18.208.94	Completed

View Datastore Details

The View Details page makes it easy to view details about a Nimble datastore. You can view details about the datastore.

Procedure

- 1 Start the vSphere client connected to vCenter.
 - 2 Click the datastore whose details to view.
- By default, the details page opens to the Status tab.



- 3 View the information of interest, including throughput, IOPS, and latency for the datastore.
 - In the Space section, the space size shows the size of the underlying volume, which is the size and the overhead.
 - The Access Control section refers to access control of Volumes and their Snapshots.
 - The volume field refers to the Nimble volume, and displays the CHAP User Name for iSCSI arrays and LUNs for Fibre Channel arrays:

Access Control			
Volume	Snapshots		
Volume	Initiator Group	Protocol	CHAP User Name
ererr0000	EsxHosts0000	iSCSI	Unrestricted Access

iSCSI

Access Control			
Volume	Snapshots		
Volume	Initiator Group	Protocol	LUN
sjc364-ds0000	EsxHosts0001	FC	0

Fibre Channel

4 Move around the tabs to view more information.

Tabs include Status, Connections, Snapshot, and Replication. If you are not sure of the datastore or action you are viewing, use the breadcrumbs at the top of the page to help you navigate.

Datacenter51	
Summary	Virtual Machines
Hosts	IP Pools
Performance	Tasks & Events
Alarms	Permissions
Maps	Storage Views
Nimble	

Datacenter51	sample
--------------	--------

Status	Connections	Snapshots	Replication
--------	-------------	-----------	-------------

Connected Initiator	# Connections
iqn.1998-01.com.vmware.virat-esx51-2-1846efea	1
iqn.1998-01.com.vmware.virat-esx51-1-71d734dc	1

For Fibre Channel, the Connections tab displays the Initiator WWPN/Alias and Target WWPN/Alias for each connection.

acceptance	FcDataStore1
------------	--------------

Status	Connections	Snapshots	Replication
--------	-------------	-----------	-------------

Connected Initiator	# Connections	Initiator WWPN	Initiator Alias	Target WWPN	Target Alias
labesx-qa02.rtplab.nimble.vmhba6	1	21:00:00:24:f4:c2:27	labesx-qa02.rtplab.nimble.vmhba6	56:c9:ce:90:ab:46:86:01	rtpl-array2-null-fc5.1-56:c9:ce:90:ab:46:86:01
labesx-qa02.rtplab.nimble.vmhba5	1				

If you have a role with appropriate permissions, you can use the icons across the top of the tab bar to perform actions on the datastore.

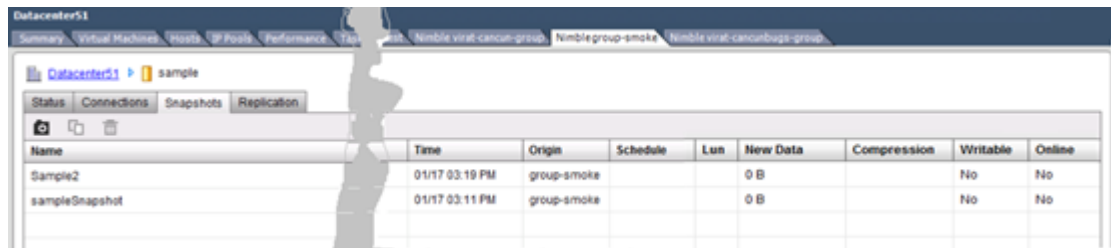
Take a Snapshot of a Nimble-based Datastore

The Nimble vCenter plugin enables you to take snapshots of VMware datastores that are mapped to volumes on the Nimble array.


Procedure

- 1 Open your vSphere client and connect to the desired datacenter.
- 2 From the list of datastores, move to the Snapshots tab and click the Nimble-based datastore containing the snapshot.

You should see a separate tab for the Nimble Datastore.



Note The image above shows the Snapshots tab for a Fibre Channel datastore, which includes a LUN field; a Snapshots tab for iSCSI datastores does not include a LUN field.


- 3 On the Datastore list view, click the Snapshot  icon or right-click and select **Snapshot...**
- 4 Provide a name and optional description for the snapshot, then click **Take Snapshot**. The snapshot now appears in the list on the Snapshots tab.

Delete a Nimble-based Datastore

The Nimble vCenter plugin enables you to delete VMware datastores that are mapped to volumes on the Nimble array.

Caution Before you delete a datastore, make sure that there is no I/O traffic or active connection to the datastore.

Procedure

- 1 Open your vSphere client and connect to the desired datacenter.
- 2 From the list of datastores available in the datacenter, click the Nimble-based datastore you want to delete.
- 3 From the list view, click the Delete  icon or right-click and select **Delete**.
- 4 Confirm that you want to delete the datastore, then click **OK**.

Unregister the vCenter Plugin Using NimbleOS CLI

If you no longer want to manage volumes on a Nimble array through a vSphere client, you can use the NimbleOS CLI to unregister the Nimble vCenter plugin from the vCenter server.

Procedure

- 1 Log into your Nimble array using the NimbleOS CLI.
See [Log in to the NimbleOS CLI](#) on page 133.
- 2 At the command prompt, type:
vmwplugin --unregister --username <username> --password <password> --server <server_hostname-address> --subnet_label <subnet_label>

Depending on which vCenter client plugin you are unregistering, add the following command option:

- **--client thick** (for desktop)
- **--client web** (for web client)

- 3 Restart the vSphere client.

Unregister the vCenter Plugin Using NimbleOS GUI

If you no longer want to manage volumes on a Nimble array through a vSphere client, you use the NimbleOS GUI to unregister the Nimble vCenter plugin from the vCenter server.

Before you begin

Ensure that none of the following are registered on the vCenter plugin that you plan to unregister:

- Web Client
- Thick Client
- VASA Provider (VVols)

Procedure

- 1 From the NimbleOS GUI main menu, select **Administration > VMware Integration**.
You see a completed registration form for each registered vCenter.
- 2 Click **Test Status** to see the current status of the plugin.
- 3 Click **Remove**.
- 4 Click **Delete**.
- 5 Click **Test Status** again to verify that the plugin has been unregistered.

Unregister the vCenter Plugin Using the vCenter Server

If you do not have access to the NimbleOS CLI or GUI, you can unregister the Nimble vCenter plugin through the vCenter server.

Procedure

- 1 In your browser address field, type:

http://<vCenter server name or IP>/mob

This action accesses the managed object browser (MOB) on the vCenter server.

- 2 Click **Content** and then select **ExtensionManager**.

There are multiple entries. Refer to the information corresponding to your vCenter desktop client plugin or web client plugin to select the correct entries to unregister.

- If unregistering the vCenter desktop client:

Look for the key entry in the format:

```
com.nimblestorage.hi.3469425087823156524
```

Identify which group the key belongs to. Open that entry and check the server information to verify that it matches the desired group.

- If unregistering the vCenter web client plugin:

Remember that all web client information is listed under a single key that uses the format:

```
com.nimblestorage.hi
```

Important Removing this single entry unregisters all groups using the web client plugin. A single group cannot be removed from the web client plugin. To re-register the vCenter web client plugin, you must register all groups again.

Do one of the following:

- To continue with unregistering all groups, remove the single entry.

- Contact Nimble Storage Support to have the entry removed for you without unregistering all groups.
- 3 Choose **UnregisterExtension**.
 - 4 Paste in the name of the plugin and click **Invoke Method**.
 - 5 Close the pop-up window.
 - 6 To verify that the Nimble vCenter plugin is no longer in the list, refresh **Managed Object Type > ManagedObjectReference > ExtensionManager**.

The Nimble vCenter Web Client Plugin

Nimble Storage provides a web client plugin that integrates with vCenter to manage datastores residing on Nimble arrays using its extension framework.

The Nimble vCenter web-based client plugin provides the same functionality as the regular vCenter desktop client plugin, with minor differences in the user interface, terminology, and feature enhancements, such as multi-group support. Nimble supports both clients, and both can be used at the same time. Using the GUI, both clients will be registered at the same time. However, if you are registering the vCenter client plugin using the CLI, only one client can be registered at a time.

Important For the vCenter web plugin, you must be running ESX 5.5 Update 1 or later, and NimbleOS 2.3.x. Only a single instance of the web client plugin can run at a time, but allows multiple group visibility.

Note If the array is in a VMware environment, best practice indicates that you have ACLs (iSCSI initiator group and/or CHAP username) on all volumes.

Register the vCenter Web Client Plugin

The web-based plugin is part of the NimbleOS. To take advantage of it, you must first register the plugin with a vCenter Server.

You can register multiple plugins on the Nimble array. Each array that registers the plugin adds a tab to the vSphere client. The tab name for the datastore page is "Nimble-<groupname>".

The vCenter web plugin is deployed the first time you log in.

You can use the CLI or GUI to register the plugin with the vCenter Server. Both the web-based vCenter plugin and the client-based plugin use the same registration steps.

To register vCenter, see [Register the vCenter Plugin Using the NimbleOS CLI](#) or [Register the vCenter Plugin Using the NimbleOS GUI](#).

See also [View a List of Installed Plugins](#).

Before you begin

Important The vCenter web client plugin is supported on ESX 5.5 update 1 and later.

Note The plugin is not supported for:

- Multiple datastores located on one LUN.
- One datastore spanning multiple LUNs.
- LUNs located on a storage device not made by Nimble.

Use a vCenter account that has sufficient privileges to install a plugin. This is usually a user assigned to the Administrator role. You need to know the vCenter hostname or IP address.

Create Roles (Role-Based Privileges)

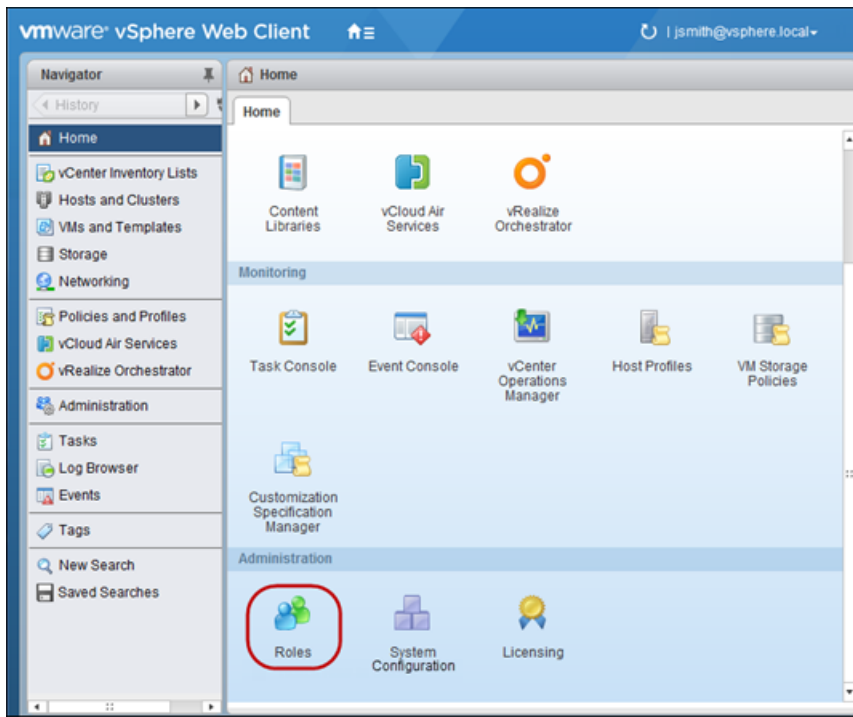
Role-based permissions protect access to Nimble-based datastores and actions taken on them.


Actions taken on Nimble-based datastores are based on roles with Nimble-specific privileges that allow or disallow features. All user roles must have a minimum of privileges listed under the Nimble Storage, Inc. privileges. There is no default role.

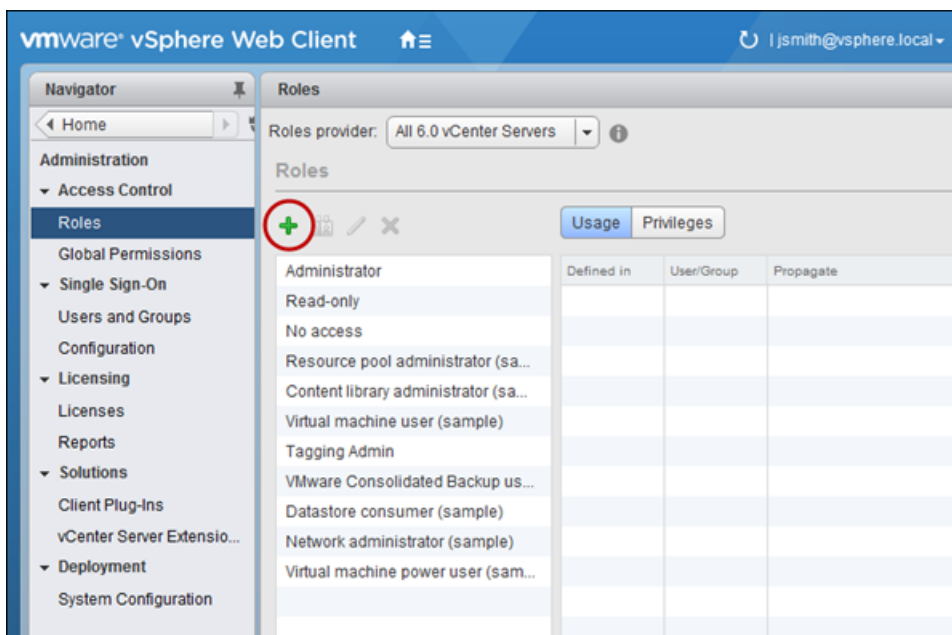
To add a role:

Procedure

- 1 Log on to the vCenter web client.
- 2 From **Home**, click **Administration** in the left navigation pane.
Alternatively, in the Home tab, under the Administration section, click **Roles**.

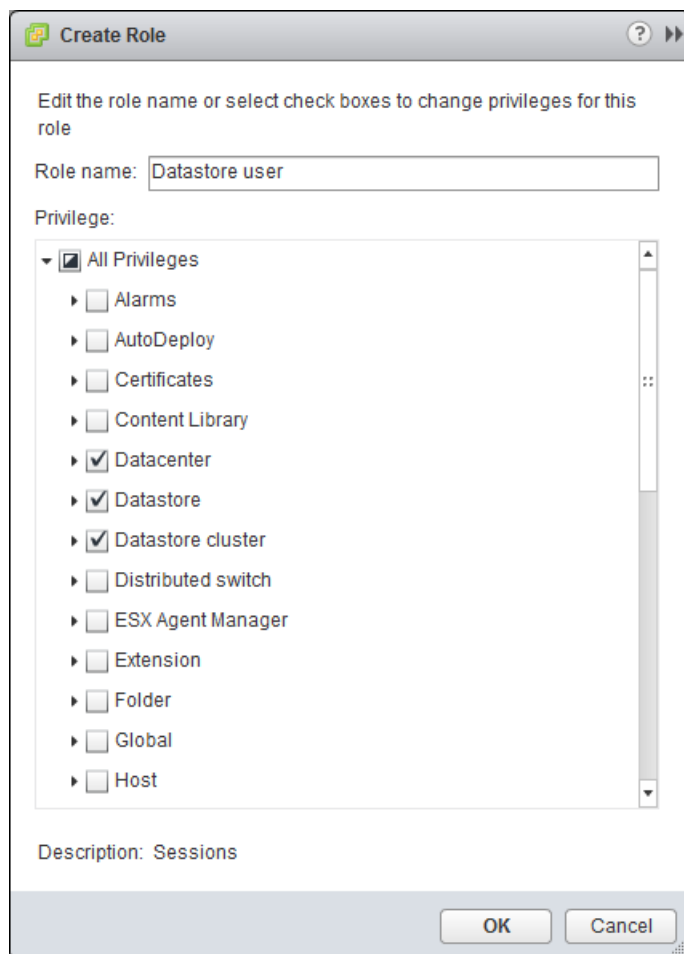


- 3 From the Roles view, click the  icon to add a user role.



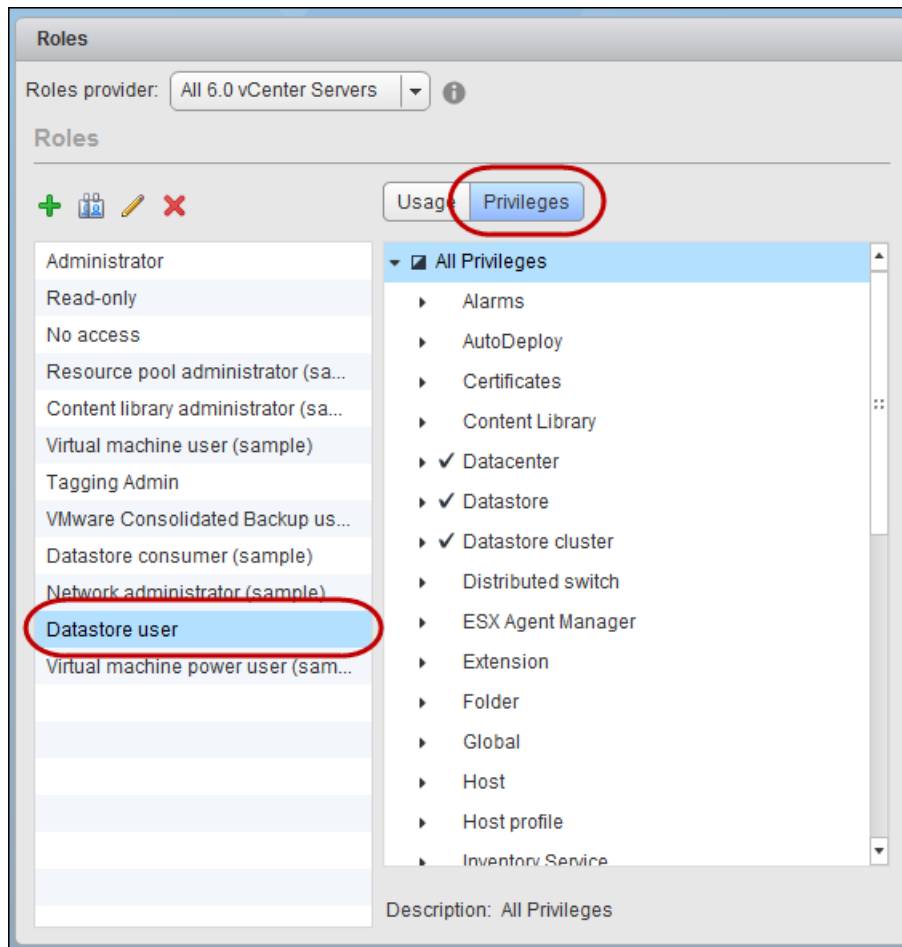
- 4 Enter a name for the new role.

Select the privileges to be associated with the role:



5 Click OK.

The newly created role appears in the list of roles. Click Privileges to view the role's associated privileges:



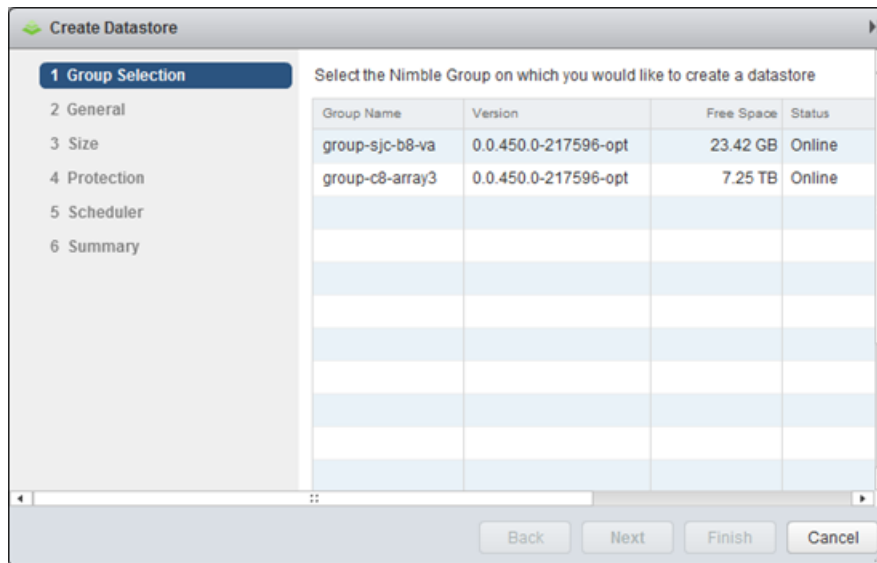
Create a New Datastore

The Nimble vCenter web plugin enables you to create VMware datastores that are mapped to volumes on the Nimble array.

To create a new datastore:

Procedure

- 1 Log on to the vSphere web client connected to vCenter.
- 2 From the Home screen, click **vCenter Inventory Lists**.
- 3 Under Resources, click **Datacenters**, and select the datacenter under which you want to create the datastore.
- 4 Right-click the datacenter and select **Nimble Storage Actions > Create Datastore** to launch the datastore wizard.
- 5 Select the Nimble group on which you want to create the datastore.



Unlike in the vCenter desktop client, a single instance of the vCenter web plugin supports multiple groups.

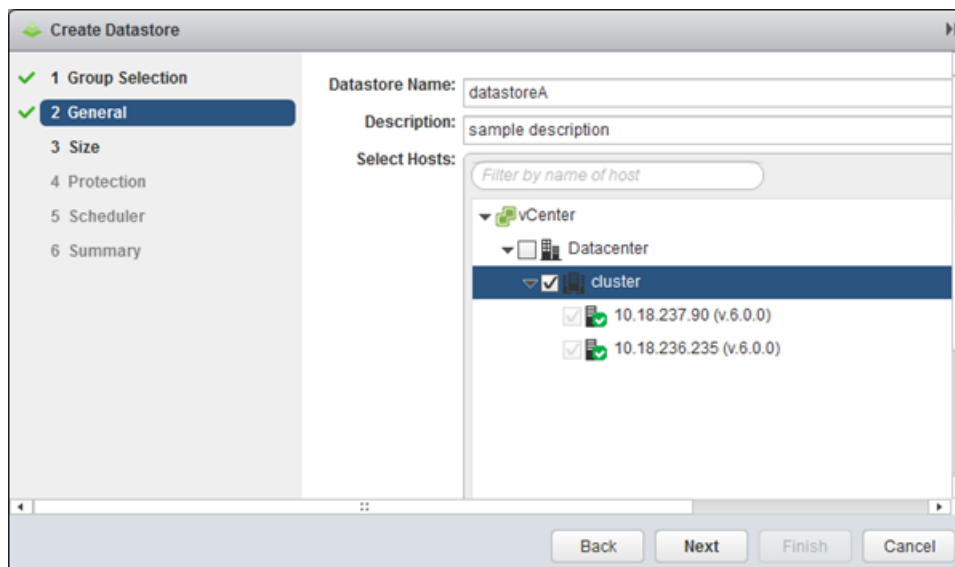
Note vCenter web plugin users must have the group-specific privilege enabled to be able to view all datastores that belong to that group.

Click **Next**.

- 6 Enter a datastore name, an optional description, and the hosts to which you want to allow access to the new datastore.

Hosts can be inside or outside of a cluster, but they must be in the same data center. If a host is within a cluster you must select the cluster, meaning that all hosts in the cluster are granted access. Offline hosts cannot be selected.

Note If the group supports Fibre Channel, only Fibre Channel hosts are listed.



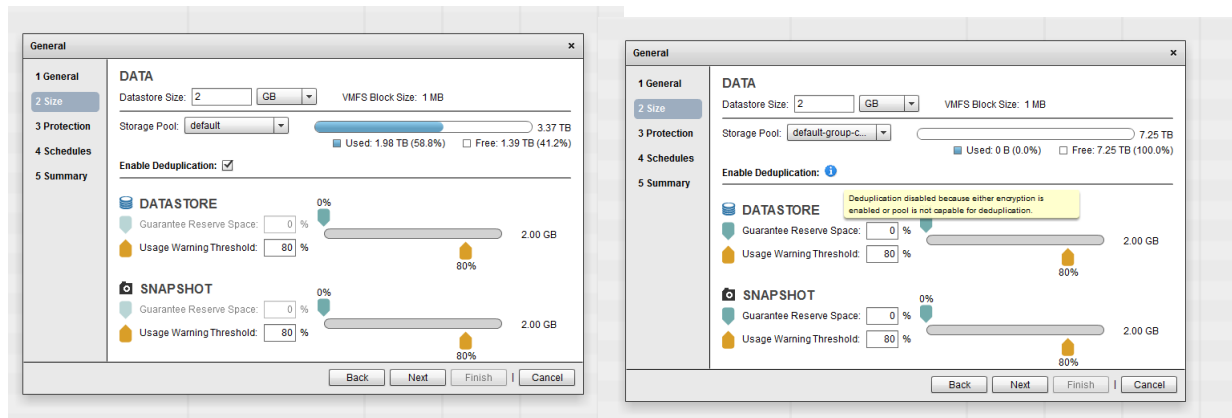
When Data Encryption is enabled on the Group or Volume, the option appears at the bottom of the General screen:



If data encryption is enabled on the Group, only the Administrator can disable it from the array, or choose to encrypt the volume. When encryption is enabled on the Volume, users with permissions can choose to enable or disable the option during datastore creation.

Click **Next**.

- Enter the desired size and space use information into the appropriate fields, then click **Next**. The graphic information below is provided as a visual cue.



Note As shown in the images above, if the pool selected is capable of deduplication, the checkbox is enabled. If the pool is not capable of deduplication, the checkbox is visible but disabled. When deduplication is checked, the datastore and snapshot reserve space is set to 0.

If all hosts are ESX 5.0 or later, VMFS 5 is used and the block size is set at 1 MB and cannot be changed. Older ESX versions use VMFS 3 and require you to set the appropriate block size.

DATA

Datastore Size: VMFS Block Size:

Storage Pool:

Used: 0 B (0.0%)

84 GB
100.0%

- Define the protection options and synchronization options, then click **Next**.

Note CHAP users must be configured on both the ESX hosts and the array.

If you enable synchronized snapshots, you must include the vCenter host and log in information. See the *Nimble Storage Administration Guide* for protection definitions.

Create Datastore

1 Group Selection
2 General
3 Size
4 Protection
5 Scheduler
6 Summary

Volume collections are used to protect datastores using similar schedules. It's recommended that you choose an existing volume collection or create a new volume collection.

☐ None
☒ Create new Volume Collection:
☐ Join existing Volume Collection:
☐ Protect as Standalone Volume

Application-consistent snapshots can be taken by enabling synchronization. To enable synchronization, please provide your vCenter credentials below.

☒ Configure synchronized snapshots

vCenter Host: 10.19.235.104 Port: 443
 User Name:
 Password:

Back Next Finish Cancel

Click **Next**.

- 9 Click **Add a Schedule** to add a new schedule to the datastore protection. Click the pencil icon (✎) to edit the schedule.

Create Datastore

1 Group Selection
2 General
3 Size
4 Protection
5 Scheduler
6 Summary

Schedule Template:

+ ✎

Name: schedule-1 Synchronization: Enabled
 Repeat: Every 1 Hours Replication: Not replicated
 Start Time: 12:00 AM
 End Time: 11:59 PM
 Days: Everyday
 Retain: 48 local snapshots

Edit

Use the calendar to create schedules, enable synchronization, and set replication levels.

Name:

Snapshots

Repeat:
 Start: :
 End: :
 Days:
 Retain: local snapshots

Synchronization

☒ Enabled ☐ Disabled

Replication

Replicate to:

✓ ✎

Click the checkmark icon to save each schedule you create. Schedule types are color-coded for easy recognition, and the legend appears at the bottom of the page. Create and add as many schedules as needed. In the list view, hover over a schedule to see a summary of the schedule, or click the schedule to see details.

Click **Next**.

- 10 View the settings summary and click **Finish**.

Caution Do not begin using the new datastore until the task finishes.

A new task appears in the task list to show you that the datastore is being created. After completion, the new datastore appears in the datastore list for the datacenter.

Mount an Existing Datastore

The Nimble vCenter web plugin enables you to mount existing datastores on new ESX hosts. There is no disruption of I/O during this operation on the datastores being mounted. The mount operation works the same way on both iSCSI and Fibre Channel arrays.

Note Datastores to be mounted must already be mounted on at least one other ESX host in the current datacenter. You cannot mount a datastore located on a different datacenter.

Procedure

- 1 Log on to the vSphere web client connected to vCenter.
- 2 From the Home screen, click **vCenter Inventory Lists**.
- 3 Under Resources, click either **Datacenters** or **ESX Cluster and ESX Host**, and select the datacenter under which you want to create the datastore.

Note

The hosts on which you can mount the datastore are determined based on how the Datastore Wizard is launched in Step 4.

- If you right click on a datacenter to launch the wizard, the datastores selected will be mounted on all ESX hosts in that datacenter.
 - If you right click on a ESX cluster to launch the wizard, the datastores selected will be mounted on all ESX hosts in that cluster.
 - If you right click on a ESX host to launch the wizard, the datastores selected will be mounted on just that ESX host.
- 4 Right-click the datacenter, ESX host, or ESX cluster, and select **Nimble Storage Actions > Mount Nimble Datastore(s)** to launch the datastore wizard.
 - 5 Select the Nimble group on which you want to mount the datastore.
Only one group can be selected at a time. Groups that do not support mounting cannot be selected.

Note vCenter web plugin users must have the group-specific privilege enabled to be able to view all datastores that belong to that group.

Click **Next**.

- 6 Select one or more datastores to be mounted.
Only datastores that vCenter can see are listed (offline volumes and datastores mounted in other datacenters are not listed).
- 7 View the settings summary and click **Finish**.

After finishing the wizard, the following takes place:

- Independent datastore tasks are created for each ESX host.
- Each task mounts the selected datastores on the hosts.


- Each task creates an initiator group per host, and adds it to the volume. Existing initiator groups are not edited.
- Mounting issues are reported on a per-host basis.

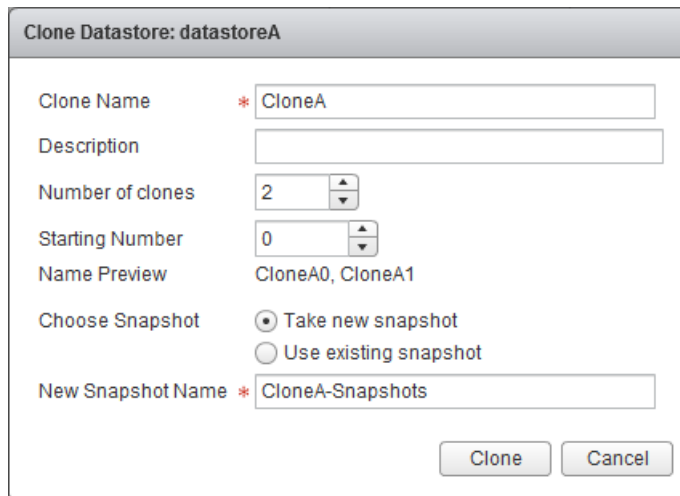
Note Because a task is created for each ESX host involved, you cannot start another mount task on that host until the current task is completed.

Clone a Datastore

The Nimble vCenter web plugin enables you to clone VMware datastores that reside on a Nimble array. Clones are created from snapshots.

Procedure

- 1 Start the vSphere web client connected to vCenter and navigate to the Datastores list view.
- 2 Right-click the datastore you want to clone and select **Nimble Storage Actions >  Clone Datastore**.
- 3 The name of the datastore to be cloned is shown at the top of the dialog box. Make sure that the correct snapshot is selected.



The dialog box titled "Clone Datastore: datastoreA" contains the following fields and controls:

- Clone Name**: A text field with a red asterisk, containing "CloneA".
- Description**: An empty text field.
- Number of clones**: A spinner box set to "2".
- Starting Number**: A spinner box set to "0".
- Name Preview**: Displays "CloneA0, CloneA1".
- Choose Snapshot**: Two radio buttons. "Take new snapshot" is selected.
- New Snapshot Name**: A text field with a red asterisk, containing "CloneA-Snapshots".
- At the bottom right are "Clone" and "Cancel" buttons.

- 4 Enter a name for the clone (required).
- 5 Select the number of clones to create.
- 6 For multiple clones, enter the **Starting number** for clones.

The Starting Number selector only appears when the number of clones is greater than one. When creating multiple clones, all clones created at this time have the same name with a number appended, for example, if the starting number is 0, the clones are named CloneA0, CloneA1, CloneA2, and so on. Clone name/numbers will be incremented from the start number. For example, if you create five clones and set the starting number to 7, the clones will be named CloneA7, CloneA8, CloneA9, and so on.

- 7 Choose to use an existing snapshot or take a new one. If you choose to use an existing snapshot, the system presents a list of snapshots for selection.
- 8 Enter a name for the new snapshot (required).
- 9 Click **Clone**.

The Active Tasks list shows an activity titled Clone Nimble Datastore and all of the subtasks.

Results

After the datastore is successfully cloned, all hosts that had mounted the original datastore also show the cloned datastore.


Grow a Datastore

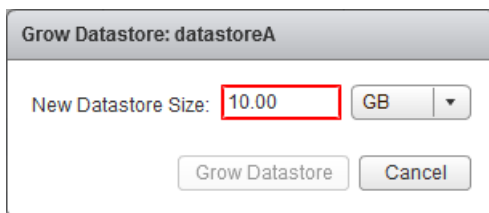
This procedure enables you to grow or resize a datastore.

If you have the correct permissions to do so, you can increase the size of a Nimble datastore.

Important To avoid selecting the wrong device during a grow operation, we recommend using the Nimble vCenter Plugin to grow any Nimble datastore.

Procedure

- 1 Start the vSphere web client connected to vCenter, and navigate to the datastores list view.
- 2 Right-click the datastore you want to grow and select **Nimble Storage Actions** >  **Grow Datastore**. The current datastore size displays. Type the new size and select the unit type.
- 3 Increase the size of the datastore to activate the **Grow Datastore** button. The minimum growth size is 1GB. This task does not allow you to shrink a datastore.

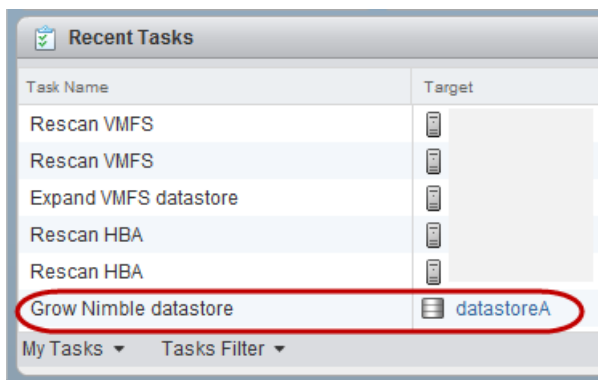


Grow Datastore: datastoreA

New Datastore Size: GB

Grow Datastore Cancel

- 4 Click **Grow Datastore**. The Active/Recent Tasks area shows the in-progress growth as a task and any subtasks.



Task Name	Target
Rescan VMFS	
Rescan VMFS	
Expand VMFS datastore	
Rescan HBA	
Rescan HBA	
Grow Nimble datastore	datastoreA

My Tasks Tasks Filter

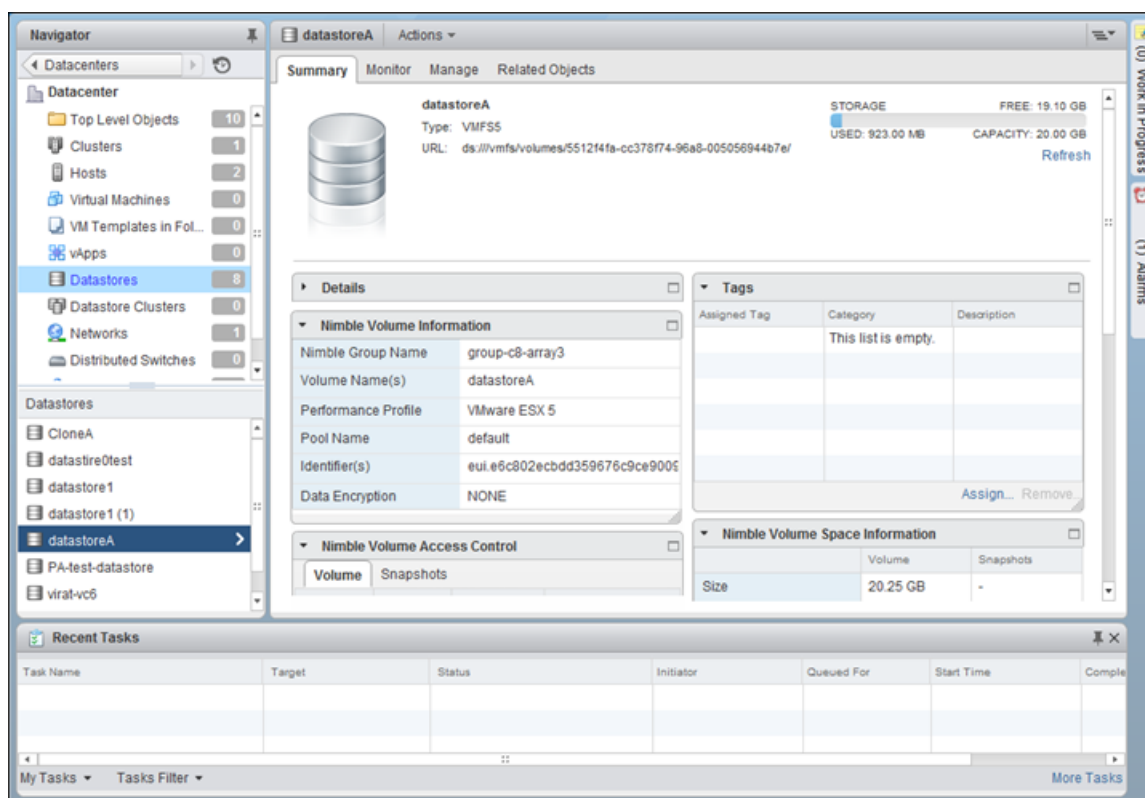
View Datastore Details

The View Details page makes it easy to view details about a Nimble datastore. You can view details about the datastore.

Note By default, the View Details privilege is not set on a datastore. If not explicitly granted, this view and its actions will be disabled.

Procedure

- 1 Start the vSphere web client connected to vCenter.
- 2 Click the datastore whose details you want to view.
By default, the details page opens to the Summary tab.



- 3 View the information of interest, including volume information, throughput, IOPS, and latency for the datastore.

There are four Nimble-related sections within the Summary tab:

- Nimble Volume Information - lists the names of the Nimble group, volume(s), pool, and gives a performance profile, identifier(s) and data encryption status
- Nimble Volume Space Information - for both volumes and snapshots: view size, usage, reserve space of the underlying volume (which is the size and the overhead), plus quota and compression data.
- Nimble Protection Policy - lists the volume collection name, synchronization data (plus access credentials), and any snapshot schedules created for the datastore
- Nimble Volume Access Control - refers to access control of Volumes and their Snapshots:
 - The Volume tab refers to the Nimble volume, and displays the CHAP User Name for iSCSI arrays and LUNs for Fibre Channel arrays:

Nimble Volume Access Control			
Volume	Snapshots		
Volume	Initiator Group	Protocol	CHAP User Name
datastoreA	ESXhost0	iSCSI	Unrestricted Access

iSCSI

Nimble Volume Access Control			
Volume	Snapshots		
Volume	Initiator Group	Protocol	LUN
datastoreB	ESXhost1	FC	0

Fibre Channel

- 4 Move around the various sections and click tabs to view more information.

Tabs include Summary, Monitor, Manage, Related Objects. Within the Monitor tab, click on an action to view Issues, Performance, Tasks, Events, Connections, and Replication. (Connections action shown):

datastoreA

Actions

Summary

Monitor

Manage

Related Objects

Issues

Performance

Tasks

Events

Connections

Replication

Connected Initiator

Connections

iqn.1998-01.com.vmware:545273bf

1

Total Initiators: 1

Total Connections: 0

Initiator IP

Target IP

For Fibre Channel, the Connections tab displays the Initiator WWPN/Alias and Target WWPN/Alias for each connection.

To perform other actions on the datastore, click **Actions** at the top of the tab bar and select a Nimble Storage Action to perform on the datastore.

Take a Snapshot of a Nimble-based Datastore

The Nimble vCenter web plugin enables you to take snapshots of VMware datastores that are mapped to volumes on the Nimble array.

Procedure

- 1 Open your vCenter web client and connect to the desired datacenter.
- 2 From the list of datastores, select the datastore to take a snapshot and click the **Manage** tab then select Snapshots and click the snapshots icon (📷), or right-click the Nimble-based datastore for which you want to create a snapshot, and select **Nimble Storage Actions > Snapshot Datastore** 📷.
- 3 Provide a name and optional description for the snapshot, then click **Take Snapshot**. Each new snapshot appears in the list under Snapshots within the Manage tab.

Name	Time	Origin	Schedule	New Data	Compression	Writable	Online
SnapshotA	03/31 02:43 PM	group-c8-array3		0 B		No	No
SnapshotB	03/31 02:42 PM	group-c8-array3		0 B		No	No
sample-schedule-	03/31 02:00 PM	group-c8-array3	schedule-1	0 B		No	No
sample-schedule-	03/31 02:00 PM	group-c8-array3	schedule-2	0 B		No	No

Edit a Nimble-based Datastore

The Nimble vCenter web plugin enables you to edit VMware datastores that are mapped to volumes on the Nimble array.

Procedure

- 1 Open your vSphere client and connect to the desired datacenter.
- 2 From the list of datastores available in the datacenter, click the Nimble-based datastore you want to edit.
- 3 Right-click the datastore, and select **Nimble Storage Actions > Edit Datastore** . The Edit Datastore wizard opens to the Size page.
- 4 Click in the text box under DATASTORE or SNAPSHOT to change reserve space or usage warning threshold percentage for the datastore itself, or snapshots taken from the datastore.

1 Size

2 Protection

3 Scheduler

4 Summary

DATA

Datastore Size: 20.00 GB VMFS Block Size: 1 MB

Storage Pool: default

Used: 90.10 GB (1.2%) Free: 7.17 TB (98.8%)

DATASTORE

Guarantee Reserve Space: 0.00 %

Usage Warning Threshold: 81.49 %

SNAPSHOT

Guarantee Reserve Space: 0.00 %

Usage Warning Threshold: 81.49 %

Back Next Finish Cancel

Click **Next** to edit protections.

- On the Protection page, select whether to create (and name), or join (and choose) an existing volume collection, or change protection to use as a Standalone volume.
If you choose to create a new volume collection, or protect the datastore as a standalone volume, decide whether to also configure synchronized snapshots, and enter the username and password for the given vCenter host.

The screenshot shows the 'Edit Datastore: datastoreA' dialog box with the 'Protection' tab selected. The left sidebar shows a progress list: 1 Size, 2 Protection (selected), 3 Scheduler, and 4 Summary. The main area contains instructions about volume collections and protection options. The 'Protect as Standalone Volume' option is selected. Below this, there is a section for 'Configure synchronized snapshots' with a checked checkbox. Fields for 'vCenter Host' (10.18.237.132), 'Port' (443), 'User Name' (vCTRuser357), and 'Password' (masked) are present. At the bottom are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

1 Size
2 Protection
3 Scheduler
4 Summary

Volume collections are used to protect datastores using similar schedules. It's recommended that you choose an existing volume collection or create a new volume collection.

☐ None
☐ Create new Volume Collection:
☐ Join existing Volume Collection: sample
☒ Protect as Standalone Volume

Application-consistent snapshots can be taken by enabling synchronization. To enable synchronization, please provide your vCenter credentials below.

☒ Configure synchronized snapshots

vCenter Host: 10.18.237.132 Port: 443
User Name: vCTRuser357
Password: *****

Back Next Finish Cancel

When finished, click **Next**.

6 View, edit, or add schedules in the Scheduler.

Click the **Calendar view** or **List view** to change how you view existing schedules. Optionally, use the drop-down to select a Schedule Template. To edit (or delete) a schedule template, hover over the schedule details box to activate the icons.

The screenshot shows the 'Edit Datastore: datastoreA' dialog box with the 'Scheduler' tab selected. The left sidebar shows a progress list: 1 Size, 2 Protection, 3 Scheduler (selected), and 4 Summary. The main area shows a 'Schedule Template' dropdown set to 'Retain-30Daily'. There is an 'Add a Schedule' button and view toggles for 'Calendar View' and 'List View'. A schedule details box for 'DAILY' is shown with fields for Name, Repeat, Start Time, Days, Retain, Synchronization, and Replication. Edit and delete icons are circled in the bottom right of the details box. At the bottom are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

1 Size
2 Protection
3 Scheduler
4 Summary

Schedule Template: Retain-30Daily

+ Add a Schedule

Calendar View List View

D DAILY

Name: daily Synchronization: Enabled
Repeat: Every 1 Days Replication: Not replicated
Start Time: 12:00 AM
Days: Everyday
Retain: 30 local snapshots

Back Next Finish Cancel

When finished editing schedules, click **Next**.

7 Finally, view a summary of your changes:

Edit Datastore: datastoreA

✓ 1 Size
✓ 2 Protection
✓ 3 Scheduler
✓ 4 Summary

Summary

Name	datastoreA
Description	sample description
Pool	default
Data Encryption	NONE

Size

Size	20.00 GB
Block Size	1 MB
Pool	default
Datastore Usage Warning	16.30 GB
Datastore Guarantee Space	0 B
Snapshot Usage Warning	16.30 GB
Snapshot Guarantee Space	0 B

Protection

Synchronization Type	VMware vCenter
Synchronization Server	10.18.237.132:443
Username	vCTRuser357

Schedules

Schedule Name	daily
Snapshot Every	1 Days
Time	12:00 AM
On the following days	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Snapshots to retain	30
Synchronization	Enabled
Replicate to	No replication partner

Back Next Finish Cancel

Click **Back** to make any further changes, or click **Finish**.

Enable iSCSI Digest

The Nimble vCenter web plugin allows you to enable iSCSI digest on a host to provide additional protection of integrity of data transferred between the host and a Nimble array.

Note If you want to add iSCSI digest parameters to volumes on VMware initiators, see [KB-000296 Enabling iSCSI Digest on VMware initiators](#).

Procedure

- 1 Login to the vSphere web client connected to vCenter.
- 2 From the Home screen, click **Storage**.
- 3 Right-click datacenter, and select **Nimble Storage Actions > Enable iSCSI Digest** to launch the wizard.
- 4 Select the Nimble group that contains the host or hosts for which you want to enable iSCSI digest.
Click **Next**. By default, all hosts in the group are selected.

- 5 Uncheck the boxes until only the required hosts are selected.
- 6 Click **Finish**.

The Recent Tasks area displays the progress and status of an activity titled Enable iSCSI Digest for Nimble SendTarget Entries.

Disable iSCSI Digest

The Nimble vCenter web plugin allows you to disable iSCSI digest on a host if you don't need the additional protection that iSCSI digest provides.

Procedure

- 1 Login to the vSphere web client connected to vCenter.
- 2 From the Home screen, click **Storage**.
- 3 Right-click the datacenter, and select **Nimble Storage Actions > Disable iSCSI Digest** to launch the wizard.
- 4 Select the Nimble group that contains the hosts for which you want to disable iSCSI digest. Click **Next**. By default, all hosts in the group are selected.
- 5 Click **Finish**.


The Recent Tasks area displays the progress and status of an activity titled Disable iSCSI Digest for Nimble SendTarget Entries.

Delete a Nimble-based Datastore

The Nimble vCenter web plugin enables you to delete VMware datastores that are mapped to volumes on the Nimble array.

Caution Before you delete a datastore, make sure that there is no I/O traffic or active connection to the datastore.

Procedure

- 1 Open your vSphere client and connect to the desired datacenter.
- 2 From the list of datastores available in the datacenter, click the Nimble-based datastore you want to delete.
- 3 Right-click the datastore, and select **Nimble Storage Actions > Delete Datastore** .
- 4 Confirm that you want to delete the datastore, then click **OK**.

Unregister vCenter Web Plugin

If you no longer want to manage volumes on a Nimble array through a vSphere client, you can unregister the Nimble vCenter web plugin.

You can unregister vCenter web plugin through vCenter, or by using the NimbleOS CLI or GUI. The steps to unregister the web client are the same as those for the client-based plugin. See [Unregister the vCenter Plugin Using NimbleOS CLI](#) on page 75 or [Unregister the vCenter Plugin Using NimbleOS GUI](#) on page 76.

If you do not have access to the NimbleOS CLI or GUI, you can unregister the Nimble vCenter plugin through the vCenter server. See [Unregister the vCenter Plugin Using the vCenter Server](#) on page 76.

Note The vCenter web plugin is removed completely only when all Nimble arrays have been unregistered from vCenter.

Virtual Volumes (VVols)

VMware virtual volumes (VVols) use VMware virtual disks mapped to a Nimble volumes. You must have vSphere 6.0 or later, ESXi 6.0 or later, and VASA Provider to use VVols. NimbleOS provides a VASA Provider you can use.

When you use VVols, you do not need to know the implementation details of the underlying storage. The Nimble storage volume resides in a VASA Provider storage container. You can use the VMware Web Client to manage the storage. All VM workflows (create, clone, snapshot, migrate, delete, HA/DRS) are supported with VVols. In addition, Nimble Storage provides analytics on the VVols through InfoSight.

How VASA Provider Works with VVols

VASA Provider uses APIs to manage VVols and to configure storage profiles that define the VVols and the Storage-Based Policy Management (SPBM). The NimbleOS contains a VASA Provider that supports VVols with Nimble arrays.

Before you can use the Nimble VASA Provider, you must register it with VMware vSphere.

Some of the advantages of VASA Provider include the ability to:

- Use SPBM to specify the storage requirements for an application. Setting SPBM ensures that the VVols used for an application have the requirements that the application needs.
- Perform periodic checks to ensure that the VVols remain compliant with the application needs.

Note If a failover occurs when you are running VASA 3.0 and your failover site has multiple storage profiles in a VMware Replication Group, some VMs are incorrectly marked as being out of compliance with the current storage profile. This is only seen when there are multiple storage profiles. It occurs because VMware checks for storage profile compliance as each VM is brought back online during the failure instead of waiting until all VVols are online and have been assigned their storage profiles.

- (VASA 3.0 and later) Provide support for disaster recovery workflows.

The disaster recovery feature included in VASA 3.0 supports VVol-based disaster recovery, not datastore-based recovery. Site Recovery Manager (SRM) and the Storage Replication Adapter (SRA) continue to support array-based recovery. See [Nimble SRM Integration](#) on page 103.

The disaster recovery feature requires that the VVols on both the source site and the target site use the same protocol. An administrator can set up a Replication Group containing specific VVols. The Replication Group, which is equivalent to Nimble Storage volume collection, represents the minimum unit of failover.

Each Replication Group resides within a Fault Domain. A Fault Domain, which is a Nimble group, specifies the set of resources that fail together. Setting Fault Domains can limit a failure because not all resources must fail together.

Protocol Endpoints

VVols are created within a storage container and are bound using a data access construct called a *protocol endpoint* (PE). All data access control is handled by the PE, which is managed automatically by NimbleOS.

PEs work in both Fibre Channel and iSCSI environments. There can be only one PE per Fibre Channel or iSCSI group. However, multiple PEs are supported in a pool. Within a Nimble group, one PE per pool is created by default when the first VVol container is created in the physical pool. The PE of a Nimble pool is shared by all vCenters and ESXi hosts that need access to the containers in that pool.

A PE is protected by an ACL that makes it visible (by iSCSI discovery and login, and FC LUN masking) to the ESXi hosts associated with the vCenter where you registered the VASA Provider. The VASA Provider creates the PE ACL entry when an ESXi host initiates communication with it. The vCenter administrator must manually add the iSCSI discovery IP to each ESXi host.

A PE is deleted when the last VVol container in the physical pool is deleted.

VVols and Nimble Connection Manager

Nimble Connection Manager (NCM) for vSphere 6.0 or later is required for VVols on iSCSI arrays. NCM supports both VVols and regular Nimble volumes. It works with all iSCSI arrays running NimbleOS version 2.x or later.

NCM manages connections to iSCSI PEs, including the following:

- Single-array or multi-array groups
- I/O path selection to VVols on multi-array pools and multiple-pool groups (without NCM, the host only establishes a connection to the PE on one pool)
- Large numbers of VVols bound by the same host
- Group-scoped iSCSI targets

NCM comprises two components: Nimble Connection Service (NCS) and Path Selection Plugin (PSP).

- NCS: Initially, NCS creates eight iSCSI sessions to the PE. This default value can be overridden by creating a `pe_sessions` parameter in the NCM configuration file - `/etc/nimble/ncm.conf`. This configuration parameter is not present by default. The minimum value for `pe_sessions` is 2 and the maximum value is 32.
- PSP: Nimble PSP uses the round-robin policy based on IOPS to switch between paths to the PE for all I/O directed to VVols. This is the same behavior used for regular Nimble volumes in a single array group.

All other components of VMware integration, such as NPM (VMware sync snapshots), vCenter Plugin, VMware Perfmetrics, and VMware Collect, are vSphere 6.0-aware and work much like they do in vSphere 5.x.

NCM is a separate online bundle. You must install it after Nimble Storage Support has enabled VVols, but before any virtual volumes are created.

Supported Features

Encryption

Encryption At Rest (EAR) is enabled at the group or volume level.

NWT

VVols allow the installation of Nimble Windows Toolkit (NWT) on a guest OS, using guest-initiated iSCSI.

Storage Policy Based Management (SPBM)

You can configure settings that define volume-level settings using SPBM. Nimble snapshots created by applying SPBM are crash-consistent snapshots.

The features that you can specify with SPBM include:

- QoS
- Performance policies
- Deduplication
- Replication
- Encryption
- Snapshots

Group and Pool Merges

VVols supports the following types of group and pool merges:

- Group merge when neither group has VVols enabled.
- Group merge when one group has VVols enabled and in use. If the group with VVols enabled is the group merged into, the operation is non-disruptive to VMs.
- Group merge when both groups have VVols enabled and in use. This operation is disruptive to VMs, as the VVols move from one VP to another.
- Adding an uninitialized array to a pool that has the VVol feature in use.
- Pool merge when neither pool has VVols in use.
- Pool merge when one of the pools has VVols in use. This operation should be non-disruptive to VMs.
- Pool merge when both pools have VVols in use. This operation should be non-disruptive and will result in two PEs in the pool.

Configuring VVols

Before configuring VVols, you must have vCenter installed. For more information, refer to the VMware vCenter installation documentation.

VVols Workflow

Follow these steps to configure VVols on your array. You must use the VMware Web Client when working with VASA Provider. These steps are described in detail in this section.

Before you begin, you should do the following:

- Before you begin, confirm that port 8443 is opened for SSL communication between ESXi hosts and Nimble Storage arrays. This port ensures that the ESXi hosts can mount the VVols databases.
- Be sure to create at least one VVol folder on the array using the NimbleOS CLI or GUI. Refer to the "Folders" section in either the *Nimble Storage CLI Administration Guide* or the *Nimble Storage GUI Administration Guide*.

Procedure

- 1 Add a vCenter Server.
- 2 Register the VASA Provider using the VMware Web Client.
- 3 Create a VVol datastore on the storage container using the VMware vSphere Web Client.

Note (iSCSI only) Configure the discovery IP address of the Nimble array. If you do not configure this IP, the Protocol Endpoints (PE) will not be visible. As a result, the VVol datastore will not be created.

- 4 Create a virtual machine using the VMware vSphere Web Client.

Note If you do not already have one, you will also need to create a VM storage policy using the VMware vSphere Web Client.

Add a vCenter Server

To use virtual volumes (VVols), you must add a vCenter server to the array. You can use either the NimbleOS GUI or CLI to add the vCenter server.

Procedure

Add a vCenter Server.

The following is an example of the NimbleOS CLI command you can use:

```
vcenter --add [--name] [--hostname {hostname|ipaddr}] [--port_number port_number] [--username
user_name] [--password password] [--description description] [--subnet_label subnet_label]
```

Register a vCenter Server Extension

To manage volumes on a Nimble array through a vCenter server, you must register a vCenter server extension with the array. You can use either the NimbleOS GUI or CLI to register the vCenter server extension. You must specify the type of extension you are registering:

- **web** for a web client
- **thick** for a desktop client
- **vasa** for a VASA Provider

Procedure

Register a vCenter server extension with an array.

The following is an example of the NimbleOS CLI command you can use:

```
vcenter --register vCenter_name [--extension {web| thick| vasa}]
```

Create a VVol Datastore

The Create Datastore wizard lets you create a VVol datastore and map it to a folder on a Nimble array. Before you can do this, you must discover the protocol endpoint (PE).

Note The folders mentioned in this task should already have been created on the array using NimbleOS GUI or CLI.

Procedure

- 1 Discover the PE.

Take the following action based on the protocol you are using:

Option	Description
An iSCSI array	Add the discovery IP and rescan.
A Fibre Channel array	Rescan.

- 2 Start the Create Datastore wizard by right clicking on **vCenter Server > Related Objects > Datastores > Create a new datastore**.
- 3 On the Type screen, choose **VVol** and click **Next**.
You see the folders created on the Nimble array.
- 4 Select the folder you want to map to the VVol and click **Next**.
You see a list of accessible hosts.
- 5 Select the host you want to map to the VVol.
- 6 Click **Finish** to complete the datastore creation process.

Create a VM

You use the VMware vSphere Web client to create a VM as well as the storage profile you want to associate with it.

Procedure

- 1 If you do not already have a storage profile, create one now using the **Create New VM Storage Policy** wizard.
 - a) From the VMware vSphere Web Client **Navigation** pane, select: **Policies and Profiles > VM Storage Policies**

- b) Click the **Create** icon.
- c) Enter the information to define the storage profile.

Note If your storage policy defines a replication line of service, choose the replication group where you want to place your VM. If you choose **Automatic**, the wizard creates a replication group for you.

2 Create the VM using the **New Virtual Machine** wizard.

From the VMware vSphere Web Client, right-click a datacenter, cluster, or host and select **New Virtual Machine** to start the wizard.

3 Enter the information required by the wizard. Most of the dialogs in the wizard are self-explanatory. Some key points when you work with the wizard include the following:

- Enter an alphanumeric name for the VM. Do **not** include any unicode characters.
- Specify a VM storage profile. Using a profile to define the VMs instead of entering the information manually helps you maintain consistency when you create new VMs.
- Select a compatible VVol datastore. Doing this ensures that Nimble volumes are created for each VMDK.

4 Click **Next**.

5 To complete the VM creation process, click **Finish**.

Managing VVols

You use the VMware vSphere Web Client to manage virtual volumes (VVols). All virtual machine workflows (create, clone, snapshot, migrate, delete, HA/DRS) are supported. The VMware documentation set contains information about these workflows. *vCenter Server and Host Management* provides an overview of these workflows and the tasks you can perform with the VMware vSphere Web Client as well as references to the documentation that describes the tasks in detail. These tasks include the following:

- Create
 - Creating Nimble volumes
- Snapshots
 - Creating Nimble snapshots
 - Restoring managed snapshots using vCenter Snapshot Manager
 - Restoring unmanaged snapshots after offlining the VM (you can also restore an unmanaged snapshot using the NimbleOS)
- Clone
 - Same container - Nimble clone
 - Different container - new Nimble volume followed by ESXi host copying data
- Migrate
 - New Nimble volume followed by ESXi host copying data
- Delete
 - Independent VVol - volume taken offline and deleted
 - Clone parent - volume taken offline and deleted when the last clone child is deleted
- Swap File Location
 - Change the location of the swap files at a host level
 - Change the location of the swap files at a cluster level

Note VVol swap volumes are not included in volume collections. It is recommended that you put the swap files into VMFS datastores to reduce the volume count requirements for VVols.

You can perform certain VVol management tasks using the NimbleOS. The *Nimble Storage GUI Administration Guide* and the *Nimble Storage CLI Administration Guide* provide detailed information about these tasks, which include the following:

- Delete/Edit/Offline a VVol
- Create/Edit/Delete a Folder
- Edit a Volume Collection

Role-Based Access Control (RBAC)

The Nimble array roles have the following access with respect to VVols:

- Administrator and Power User
 - Can perform all operations - create, read, update, and delete
 - No buttons or menus are hidden
- Operator
 - Can perform create, read, and update operations
 - Can not delete a vCenter instance, so the **Remove** button is hidden on the vCenter page.
- Guest
 - Allowed to view only the vCenter page
 - Can not perform create, update, or delete operations
 - The **Add new vCenter**, **Edit**, and **Remove** buttons are hidden on the vCenter page.

Note A **vcenter** command allows you to manage Nimble's VMware vCenter extensions, and add, edit, and delete a vCenter appserver. For more information, refer to the *Nimble Storage Command Reference*.

Using VASA Provider to provide disaster recovery for VVols

VASA 3.0 includes a VVol-based disaster recovery feature. It requires an upstream (protected) site and a downstream (recovery) site. You can use the VMware vSphere Web Client to enable this feature.

Before you begin

You must have set up your upstream and downstream sites. Each site must have the following:

- A vCenter Server
- Note** Both sites (upstream and downstream) must be running the same version of vCenter Server.
- A VASA Provider that is running VASA 3.0
 - A VVol datastore that resides within the vCenter Server

Procedure

- 1 Mount the destination folder as a VVol datastore within the downstream site vCenter Server.

Tip It is a good practice to use the same name for both the upstream folder and the downstream folder.

- 2 Click the checkbox to make the association between the upstream and downstream folders.

After you do this, the defined partner will be listed in the storage profile configuration wizard within the VMware vSphere Web Client.

- 3 Use the Web Client to define your storage profile and configure the VMware replication line of service.

Troubleshooting Tips

This section describes the most common issues and their resolutions/workarounds.

Registration Error - Invalid Provider Certificate

You see the message "The provider certificate is invalid. It is either empty, malformed, or expired, not yet valid, revoked, or fails host name verification."

Procedure

- First, try clicking **OK** again.
- If you still see this message, it may be that the certificate is invalid. This error indicates the address used in the URL is not in the certificate, or that the certificate start time is in future (compared to vCenter's current time).

Failure to Add VP - Time Mismatch

You see a "Failure to Add VP - Time Mismatch" error.

This could be due to a time mismatch between vCenter and the array. Check the following timestamps in the order presented below.

- 1 First, look at the current time on vCenter.

```
# date
Thu Dec 18 15:10:56 UTC 2014
```

- 2 Then look at the current time on the array. In this example the time is different.

```
# date --utc
Thu Dec 18 15:15:37 UTC 2014
```

- 3 Then look at the certificate start time in UTC. In this example, the start date and time cannot be before December 18 at 16:58. The current times on vCenter and the array, in these examples, are earlier than the certificate start time.

```
#
openssl x509 -in /nimble/var/private/config/current/group/certs/host.crt
-noout
-startdate notBefore=Dec 18 00:16:58 2014 GMT
```

- 4 Then look at errors in vCenter sps.log. In the example below, the timestamp check has failed because of the above conditions.

```
# grep "timestamp check failed"
/var/log/vmware/vmware-sps/sps.log 2014-11-26 06:02:44,628
[pool-14-thread-3]
WARN opId=4106403a-680d-4cd4-80d2-8e7e66d9762a
com.vmware.vim.sms.provider.vasa.VersionHandler - [isLegacyProvider]
Failed to retrieve version information from provider:
sun.security.validator.ValidatorException: PKIX path validation failed:
java.security.cert.CertPathValidatorException: timestamp check failed
```

- 5 Finally, look for errors in vvolld.log on ESXi. The example below, the certificate is not yet valid.

```
2014-12-17T17:41:37.154Z error vvolld[FFD2FB70] [Originator@6876
sub=HttpConnectionPool-000000] [ConnectComplete] Connect failed to <cs
p:1f26bdc8, TCP:10.18.112.46:8443>; cnx: (null), error:
N7Vmacore3Ssl18SSLVerifyExceptionE(SSL Exception: Verification parameters
```

Procedure

- Synchronize the times on vCenter and on the array.

Datastore Inaccessible

If the datastore is inaccessible, there are three things to check:

Procedure

- For an iSCSI array, check to see if the discovery IP is configured on the ESX hosts.
A static target with a group name should show up after performing a rescan.
- Ensure that the ESX time is not behind the array time.
See [Failure to Add VP - Time Mismatch](#).
- Ensure that the latest version of NCM is installed on every host that should mount the datastore.

Nimble SRM Integration

The VMware vCenter Site Recovery Manager (SRM) is a plugin to the vCenter Server that enables you to create and test disaster recovery plans in a VMware environment.

The Nimble Storage Replication Adapter (SRA) enables a Nimble array to support SRM and function in a VMware environment. SRM and SRA enable you to perform an array-based recovery.

Note VASA Providers that use VASA 3.0 also provide a disaster recovery feature that restores virtual volumes (VVols). This feature supports a VVol -based disaster recovery, not a datastore-based recovery. See [How VASA Provider Works with VVols](#) on page 95.

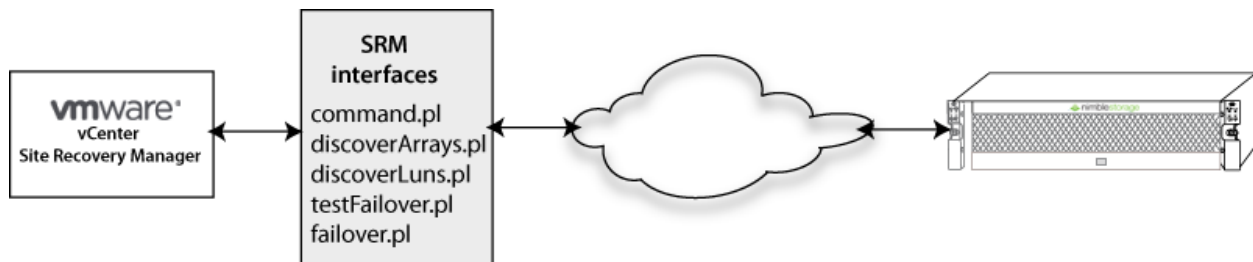
How SRA works with SRM

Using Nimble Storage Replication Adapter (SRA) with the VMware vCenter Site Recovery Manager (SRM) enables you to create and test a Disaster Recovery (DR) plan based on a Nimble array without affecting your production environment. After you verify that your DR plan works the way you expect, you know that your DR plan is adequate to protect your datacenter.

In DR scenarios, your DR replication partner (Nimble array) maintains your data for immediate availability.

The Nimble array uses the VMware-provided interfaces to talk to the VMware vCenter SRM using TCP/IP.

The following block diagram shows how the Nimble SRA communicates with the VMware vCenter SRM.



See [Site Recovery Manager Installation and Configuration](#) and see [Site Recovery Manager Administration](#) from VMware for instructions about how to set up and configure SRM. [VMware KB 1014610](#) also contains information about how to set up Site Recovery Manager with partner storage arrays while the [VMware vSphere Blog](#) provides SRM setup videos.

Note Do not use wildcards to configure an initiator group IQN that is used as part of an SRM configuration.

Overview of SRA Setup Process

Setting up Nimble Storage Replication Adapter (SRA) for Site Recovery Manager (SRM) involves performing steps on the SRM Server, the vCenter Server, the ESXi host, and the NimbleOS array. Detailed information about these tasks is available in the following documentation:

- SRM. See the VMware SRM documentation, including [Site Recovery Manager Installation and Configuration](#), [Site Recovery Manager Administration](#), [VMware KB 1014610](#), and [VMware vSphere Blog](#).
- NimbleOS array. See the NimbleOS Administration Guides that are available on InfoSight in the [Documentation](#) section.
- vCenter Server and ESXi. See the VMware documentation for these products.
- SRA. Information about working with SRA is provided in this document.

The steps that follow provide a high-level overview of the actions you must perform and where you must perform them so that you can plan your installation and setup. These steps are a checklist of the actions you must take and do **not** contain all the details necessary to perform the steps. See the appropriate documentation for detailed instructions.

- 1 **(SRM Server)** Install SRM. You must install SRM before you can install SRA.
- 2 **(SRM Server)** Install SRA.
- 3 **(NimbleOS)** Set up replication partners on the NimbleOS arrays.
 - a Set up at least one array in a group for the upstream (protected) site and another array in a group for the downstream (recovery) site.
 - b Use the wizard to pair the two groups as replication partners in NimbleOS: **Nimble UI > Manage > Replication > Replication Partners > New Replication Partner**
- 4 **(NimbleOS)** Create initiator groups. You must create an initiator group on the upstream protected site. You do not need to create one on the downstream site unless that array has production VMs that must be included in an SRM workflow, or you want to limit access to a placeholder volume.

Use the wizard to create the initiator groups in NimbleOS: **Nimble UI > Manage > Initiator Groups > Create**

Note Using a wildcard or leaving the IQN field blank will result in an error. An initiator group must include an IQN for each resource mapping relationship.
- 5 **(NimbleOS)** Set up one or more volume collections on the upstream Nimble array. If the downstream array is hosting production VMs, you must make sure all volume collections are replicated there.

Use the wizard to set up volume collection in NimbleOS: **Nimble UI > Manage > Protection > Volume Collection > New Volume Collection**
- 6 **(NimbleOS)** Create the following volumes:
 - A Datastore Volume at the upstream production site to store the VMs you have set up to be protected.
 - A Placeholder Volume at both the upstream and downstream site to hold the placeholder VMs prior to a recovery operation but after a protection group is created

Use the wizard to create these volumes. You must run the wizard twice to set up both volumes. **Nimble UI > Manage > New Volume**
- 7 **(ESXi)** Make sure the protocol you are using is set up correctly:
 - FC environment. You must have proper zoning in place so that a rescan of the HBAs will allow SRM to discover the recovered volume.
 - iSCSI environment. You must make sure that the recovery ESXi hosts are logged into the downstream array. Use the vCenter Server wizard to set up the software iSCSI Adapter: **VMware vSphere Web Client > Hosts and Clusters > <Your_ESXi_Host> > Manage > Storage > Storage Adapters > Add New Storage Adapter > Software iSCSI Adapter**
- 8 **(ESXi)** Mount the Datastore volume on the upstream site and Placeholder volumes on the upstream and downstream sites. You can use the wizard to do this: **VMware vSphere Web Client > Hosts and Clusters > <Your_ESXi_Host> > Related Objects > Datastores > Create a New Datastore**
- 9 **(SRM Server)** Configure the Array Manager to enable array-based replication on each site in the SRM. You add arrays at the Nimble Array Group level. If you have multiple arrays in a group, you only need to add the group once.

You can use the wizard to do this: **VMware vSphere Web Client > Home > Site Recovery > Array based Replication > Objects > Add New Array Manager**
- 10 **(SRM Server)** If you did not pair the arrays using the Array Manager wizard, you can pair them now using the wizard: **VMware vSphere Web Client > Home > Site Recovery > Array based Replication > <Select an Array> > Manage > Array Pairs**

Select the array pair from the list and click **Enable Array Pair**.

11 (SRM Server) Pair the vCenter Server sites. You can use the wizard to do this: **VMware vSphere Web Client > Home > Site Recovery > Sites > <local Site> > Pair Site**

12 (SRM Server) SRM has a built-in set of mappings to control the networks, folders, hosts or clusters, and storage policies that the VMs will use as well as the datastores that are used for placeholder files. You can use SRM to create reverse relationships automatically. You perform these actions by going to **VMware vSphere Web Client > Home > Site Recovery > Sites > <Select Site> > Manage**

For more information about working with these settings, see the SRM documentation.

SRA for SRM Prerequisites

While different versions of Nimble Storage Replication Adapter (SRA) for Site Recovery Manager (SRM) have different requirements and prerequisites, there are also some shared prerequisites:

- VMware SRM must be installed before you install SRA. In addition, you must have administrator privileges on the SRM server.
- Both the upstream and downstream replication sites must be running the same version of vCenter Server.
- **Note** You can mix vCenter Application and Standard vCenter Server on Windows.
- You must install the same version of SRA on both sites.
- Both sites must be able to communicate with both SRM, SRA, and the NimbleOS arrays.
- All VMs affected by this must be mounted to ESXi hosts.
- Protocol requirements:
 - iSCSI environments: The recovery ESXi hosts must be logged into the destination array.
 - FC environments: Zoning must be set up so that a rescan of the HBAs allows SRM to discover the recovered volumes.
- (Recommended) Install Nimble Connection Manager on each ESXi host that has a relationship with a Nimble volume.

For specific information about SRA requirements for different SRA versions, see the *Validated Configuration Matrix*, which is posted on [InfoSight](#) (**Resources > Documentation**).

For information about SRM, see [Site Recovery Manager Installation and Configuration](#).

Download the SRA for SRM Installation Package

You must download the Nimble SRA for SRM software from the InfoSight portal. You can place the downloaded file on the Windows or Linux host where you plan to install SRA.

Procedure

- 1 Go to <https://infosight.nimblestorage.com/>.
- 2 Click the **Login** link and enter your login ID and password.
- 3 Select **Resources > Software Downloads**.
- 4 In the Integration Kits section on the left side of the page, select **Storage Replication Adapter (SRA) for SRM**.

The installation package has a name similar to "Nimble_SRA_x.x.x.x.zip"

Where x-x-x-x is the SRA version number.

- 5 Extract the Nimble_SRA_x.x.x.x.zip file to access the Nimble-SRA-x.x.x.x.exe installer file.

Install SRA for SRM

Before you begin

Before you install and set up Nimble Storage Replication Adapter (SRA) for Site Recovery Manager (SRM), you must have:

- Met the prerequisites for Nimble SRA for SRM. SRA for SRM Prerequisites
See [SRA for SRM Prerequisites](#) on page 105.
- Installed and begun running a version of VMware SRM that is compatible with the version of SRA you plan to install.
- Ensured that you will install the same version of SRA on both the upstream (protected) and the downstream (recovery) sites. This version of SRA must be compatible with the currently installed versions of SRM and NimbleOS.
- Ensured that both sites allow communication between the arrays for the purpose of replication.
- Obtained the Nimble SRA for SRM installation file from the Nimble Storage InfoSight portal and extracted the SRA installer file.

See [Download the SRA for SRM Installation Package](#) on page 105.

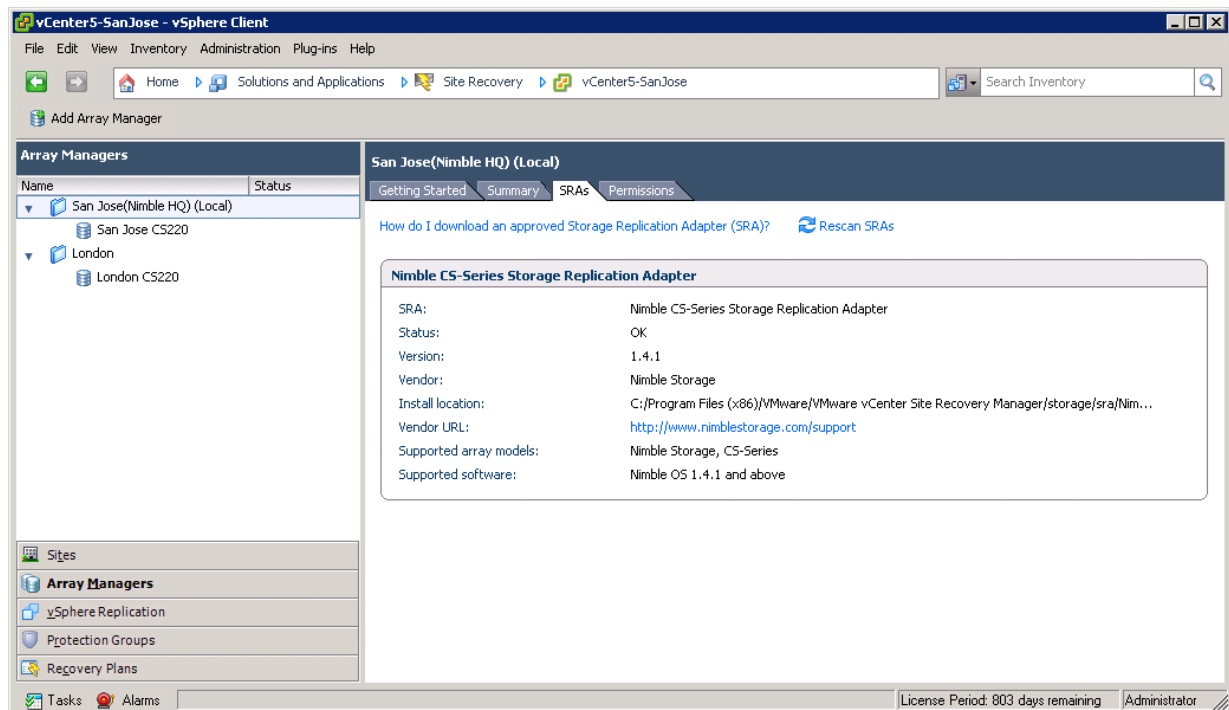
Procedure

To install Nimble SRA for SRM:

- 1 Log into the SRM server with administrator privileges.
- 2 Right-click the Nimble SRA for SRM installer file and select **Run as administrator**.
This starts the Nimble SRA - InstallShield Wizard.
- 3 Follow the steps in the wizard.
These steps are self-explanatory.
You must install SRA on both the upstream and downstream sites.
- 4 When the wizard completes, log into the SRM GUI to refresh the newly installed instances of SRA.
Select the following:

vCenter Home > Site Recovery > Sites > <your_SRA_site> > Monitor > SRAs > Refresh Button

SRA alerts you if it detects a compatible SRA installation at the remote site. If the sites are paired and have SRA installed on each one, you might have to go to the remote site and select **Refresh** before the status update occurs.



Update SRA for SRM

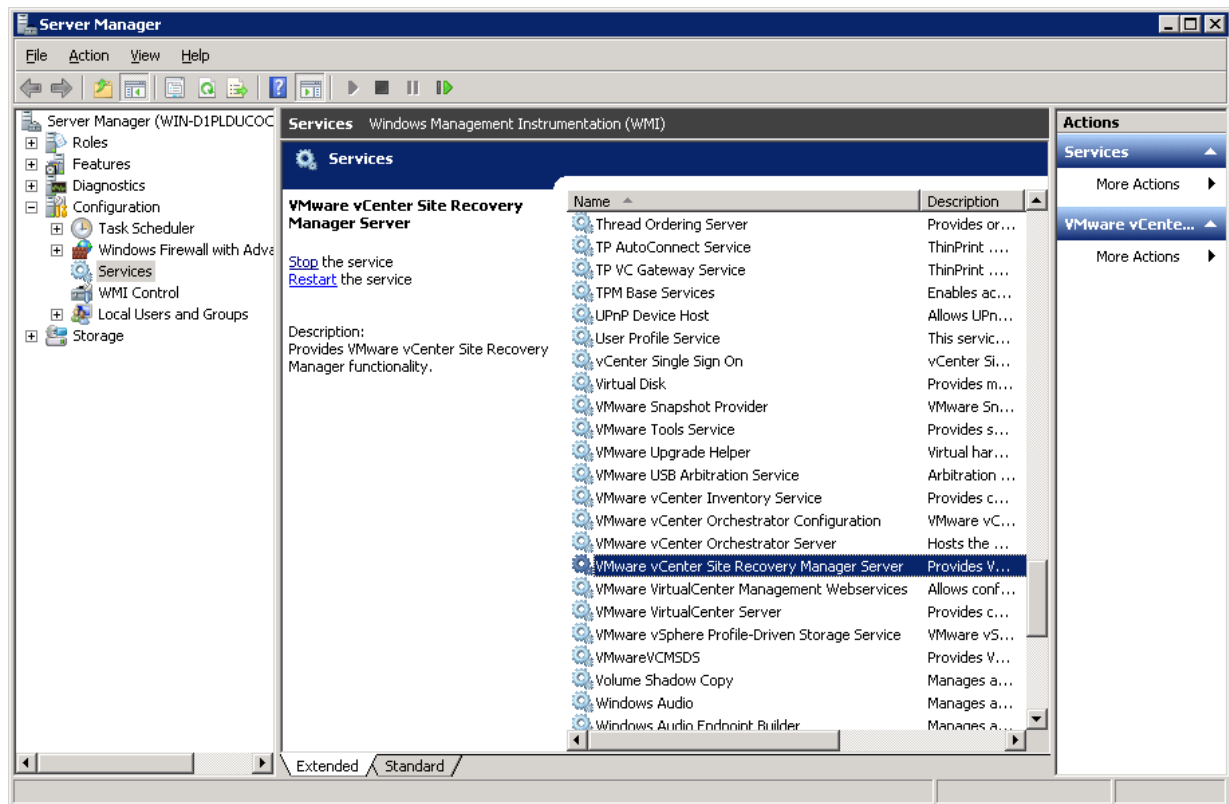
When you update Nimble Storage Replication Adapter (SRA) for Site Recovery Manager (SRM) on the Windows host, you install a full version of Nimble SRA for SRM on top of an existing installation. You can install the update without un-installing the current version of Nimble SRA for SRM.

Before you begin

To update Nimble SRA for SRM, you must have the downloaded Nimble SRA for SRM installation package. See [Download the SRA for SRM Installation Package](#) on page 105.

Procedure

- 1 Check to make sure that no SRM operation is running.
- 2 Double-click the downloaded Nimble SRA installer file and follow the prompts through the Windows Installer.
- 3 From the Windows Services, highlight *VMware vCenter Site Recovery Manager Server*, and click **Restart**.

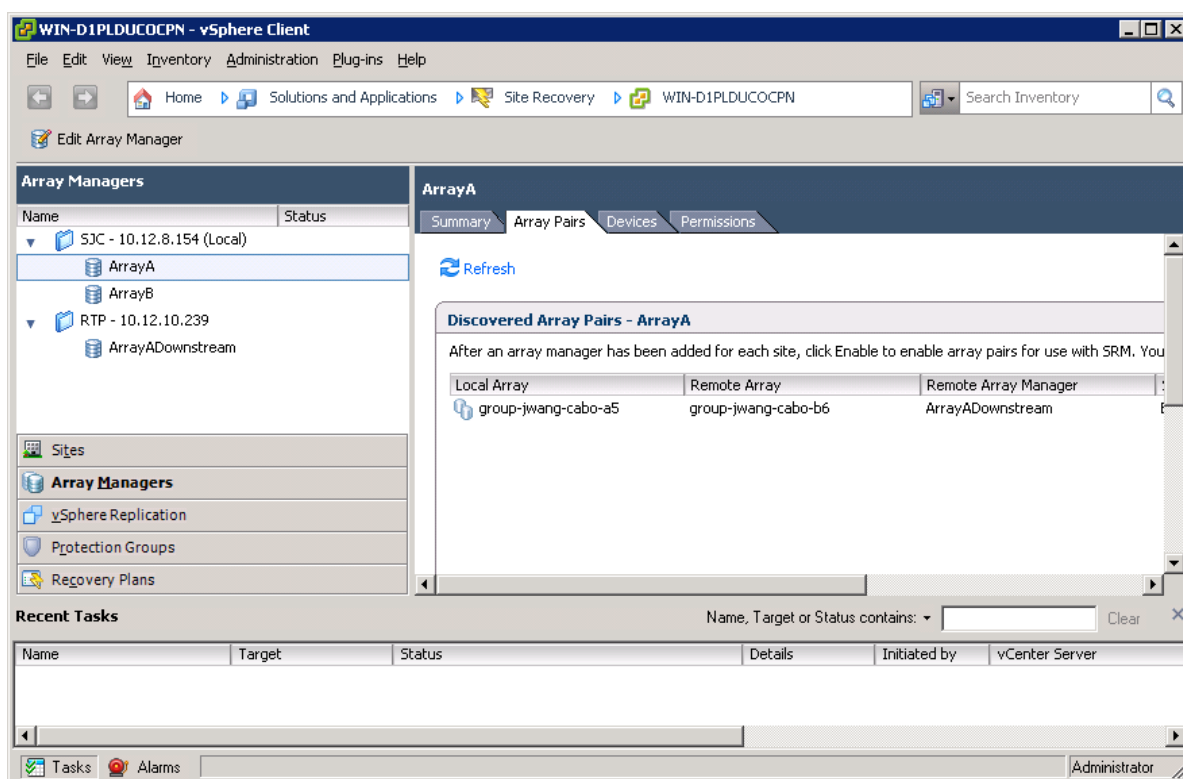


4 Verify that the update was successful.

- Make sure that there are no errors displayed in the existing Array Manager.
- In the vSphere Client, click **Edit Array Manager**.
- Make sure that only a Local Array is specified in the connection specification.

Previously, SRA required both Local Array and Remote Array connection specifications. There is no need to re-enter the Username and Password.

- Click **Cancel**.
- In the vSphere Client, under the Array Pairs tab, click **Refresh**.
- Make sure that no errors are reported.



Un-install SRA for SRM

If you find that you need to un-install the SRA for any reason, use this process.

This procedure applies to Nimble SRA for SRM 5.0, 5.1, 5.5, and 6.0.

Procedure

To un-install Nimble SRA for SRM from the ESXi server:

- 1 Log into the ESXi server as the administrator.
- 2 Right-click the setup icon or use **Control Panel > Programs** to find the SRA.
- 3 Right-click the SRA and select **Remove** from the menu or click **Uninstall** from the Control Panel.
- 4 Confirm removal if requested.

Configuring SRM and SRA to work with Nimble storage arrays

You must configure array-based replication in Site Recovery Manager (SRM) for each site. Arrays are added at the Nimble Array Group level. You only need to add the group once, even if you have multiple arrays in it. Depending on the version and your setup, the exact configuration steps might differ slightly from the following ones. See the VMware SRM documentation for specific information.

Before you begin

You must have logged into SRM and refreshed each instance of Nimble Storage Replication Adapter (SRA) for Site Recovery Manager before you begin.

Procedure

- 1 From the **Home** page of the VMware vSphere Web Client, select **Site Recovery > Array Based Replication > Objects**.

- 2 Click the **Add New Array Manager** icon.

- 3 When the **Add Array Manager** wizard starts, supply the information it requests.

Most of the information required by the wizard is self-explanatory. Some points to keep in mind as you supply information on the different panes of the wizard include the following:

- **Options pane:** You must have a pair of array managers. You can use the wizard to configure them both at once, or you can configure one array manager for one site and then repeat the process for the other site.
- **Location pane:** You must select the site where the array you are currently configuring is installed.
- **Select SRA type pane:** You can only associate one version of SRA with an array. If you have multiple versions of SRA installed, you must select the version that you want associated with this array.
- **Configure array manager pane:** This pane provides several options for configuring the array associated with the upstream site. Some of the best practices for these fields include the following:
 - **Display Name:** For consistency, use the same name here as the name of the Nimble Array group.
 - **IP Address of Local Array:** This is the group management IP address of the Nimble Array Group you are adding.
 - **Username and Password:** This is the username and password required to manage the Nimble Group. Most sites use the username and password for the **admin** user.
- **Configure paired array manager pane:** This pane is only visible if you are configuring a pair of array managers. It enables you to configure the array associated with the downstream site. You supply the same information that you entered for the upstream site in the **Configure array manager pane**.
- **Enable array pairs pane:** If you are configuring two arrays at once, you select them here. If you are adding a single array, you can use this pane only if you have already registered the partner array to the other site. Otherwise, you must skip this pane.

- 4 Review your configuration. If it is correct, select **Finish**.

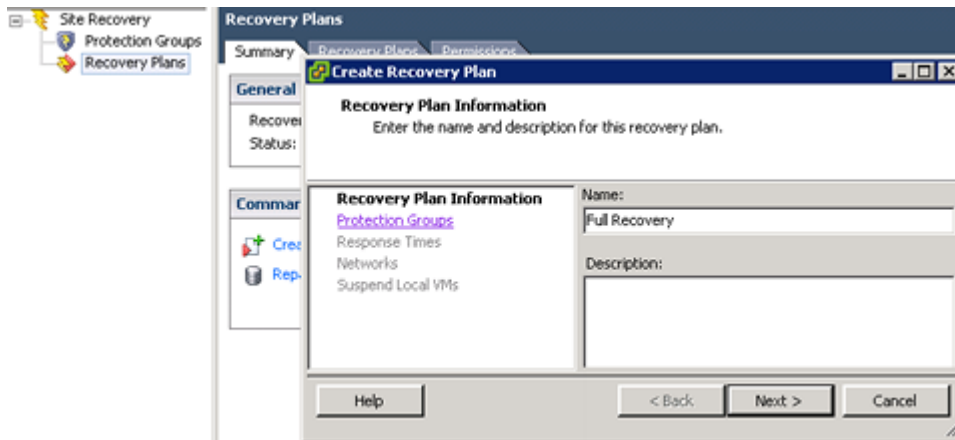
You must complete these steps for each Nimble Array Group in the Site Recovery Manager configuration.

Initiate a Recovery Plan

If your primary (protected) site goes down, you must initiate a recovery to ensure business continuity. That action requires that you have a recovery plan, preferably one created on VMware vCenter Site Recovery Manager (SRM).

In case of a site failure, you can make data in your volume collections available to applications from the replica array while you restore the failed array.

In the vCenter SRM, click the Recovery Plans tab to begin creating your recovery plan.



For more information, see [Site Recovery Manager Installation and Configuration](#) and see [Site Recovery Manager Administration](#) from VMware.

Test the Recovery Plan

Refer to the [Site Recovery Manager Administration](#) from VMware to:

- Configure protection groups on the protected site
- Create a recovery plan at the recovery site

Note Nimble SRA for SRM must be installed on your host.

Procedure

To test your recovery plan:

- 1 Connect to SRM through the vCenter client.
- 2 Run the SRM Test Recovery Plan in test mode.
- 3 To end the test, click **Cleanup**.

Results

The Nimble SRA for SRM performs the necessary cleanup after the test recovery has been performed.

Implement the Recovery Plan

The vCenter Site Recovery Manager (SRM) lets you respond quickly when a site goes down.

After a site failure, you can make data in the volume collections available to applications from the replica while you restore the failed controller shelf. Once the failed controller shelf is restored or replaced, you can return data I/Os to the original partner and restore the relationship with downstream partner at the DR site.

VMware SRM 5.0 introduced the *Reprotect* operation to configure protection in the reverse direction automatically. Reprotect helps in preparation for failback to the primary site.

Before you begin

There must be a [recovery plan](#) previously created in vCenter SRM.

Refer to [Site Recovery Manager Administration](#) from VMware.

Procedure

To implement the recovery plan:

- 1 Connect to SRM through the vCenter client.
- 2 Use the VMware SRM Run Recovery Plan feature.
- 3 When the primary site is replaced, create and test a new recovery plan in SRM.

In this case, failing over is equivalent to failing back.

Usage of Nimble SRA with Microsoft Volume Shadow Service (VSS)

VSS enables application-consistent snapshot and recovery of Microsoft Exchange and SQL Database servers. The virtual storage of these applications can be connected by either Raw Device Mapping (RDM), VMDK or In-guest Attached iSCSI. Each of these connectivity options requires different design considerations to be used with Nimble SRA. For details on the design considerations, refer to the *VMware Site Recovery Manager and Nimble Storage* best practices guide.

Helpful Information

The following pages contain helpful information about the Nimble array.

Most of these functions are handled automatically by Nimble Connection Manager (NCM). These procedures are supplied for installations where NCM was not installed or you prefer to make these settings manually.

Configure iSCSI Discovery

Before you begin

This procedure assumes you have created volumes on a Nimble array and set up any required initiator groups for access control.

If you want to configure iSCSI Digest, see the following:

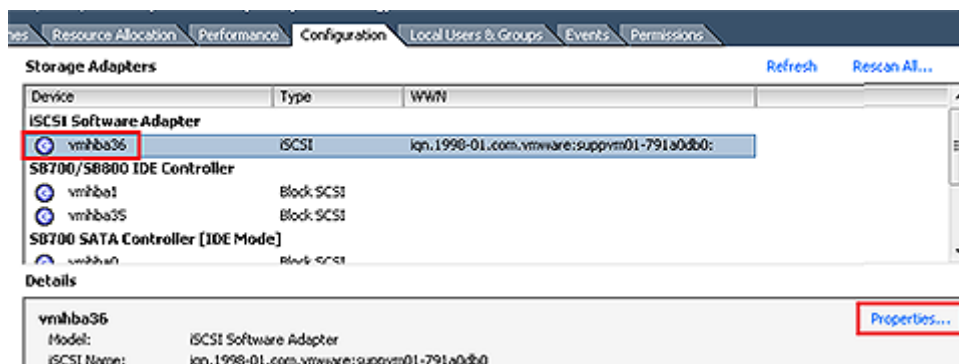
- [Enable iSCSI Digest](#) on page 93
- [KB-000296 Enabling iSCSI Digest on VMware initiators](#)

Important Validated configurations involving iSCSI hardware adapters are limited. See the *Validated Configuration Matrix* for information about configurations that have been tested.

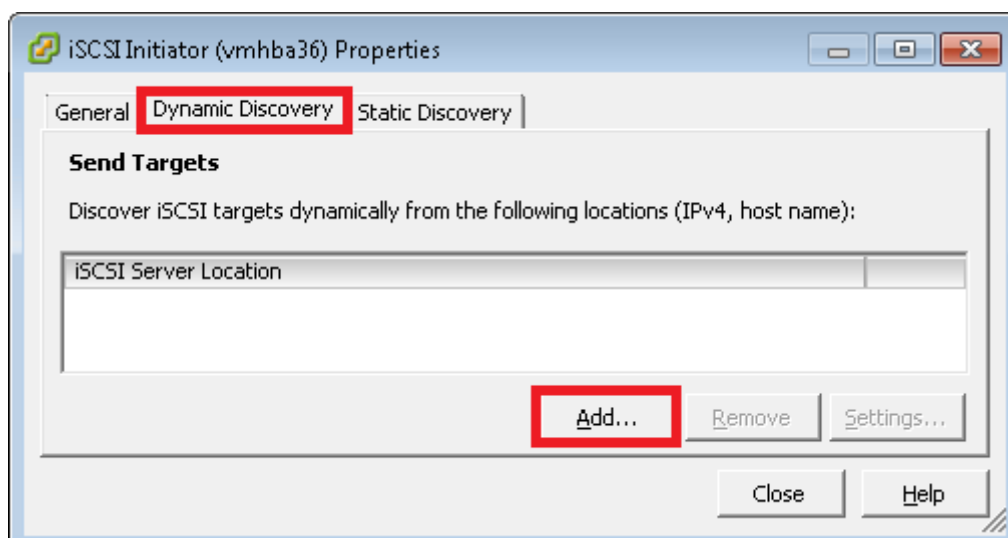
Procedure

To configure the ESXi iSCSI software adapter to discover iSCSI targets on a Nimble array:

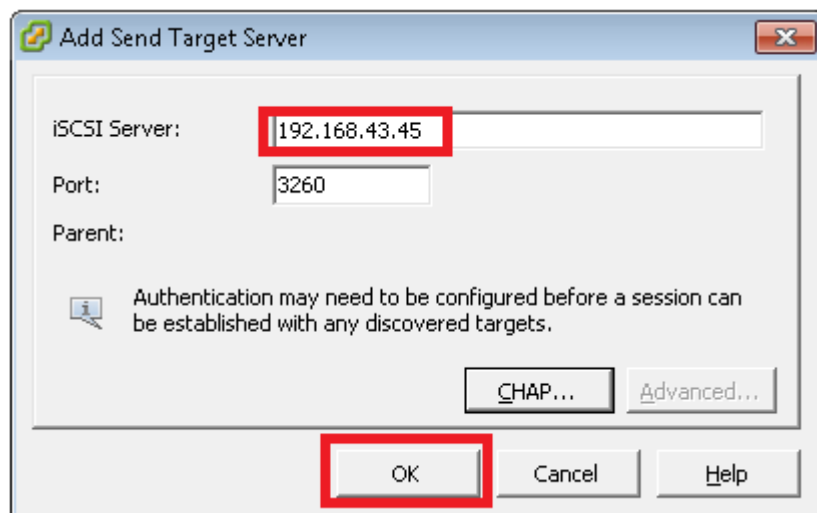
- 1 From the Configuration / Storage Adapters screen on the ESXi host, select the iSCSI Software Adapter and click **Properties**.



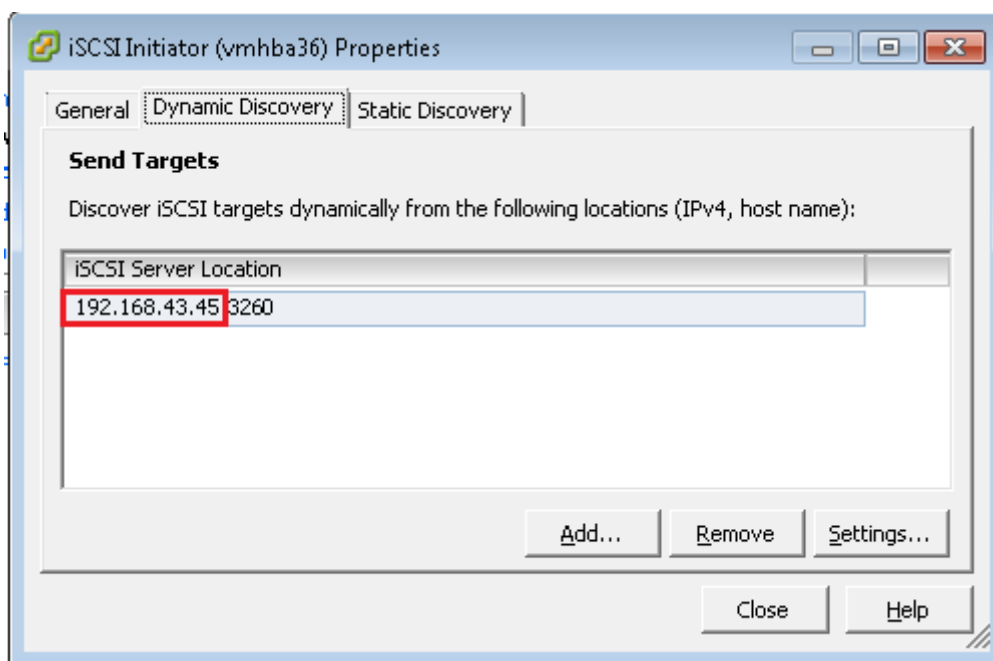
- 2 Go to the Dynamic Discovery tab and click **Add**.



- 3 Enter the Discovery IP address of the Nimble array in the iSCSI Server field and click **OK**.



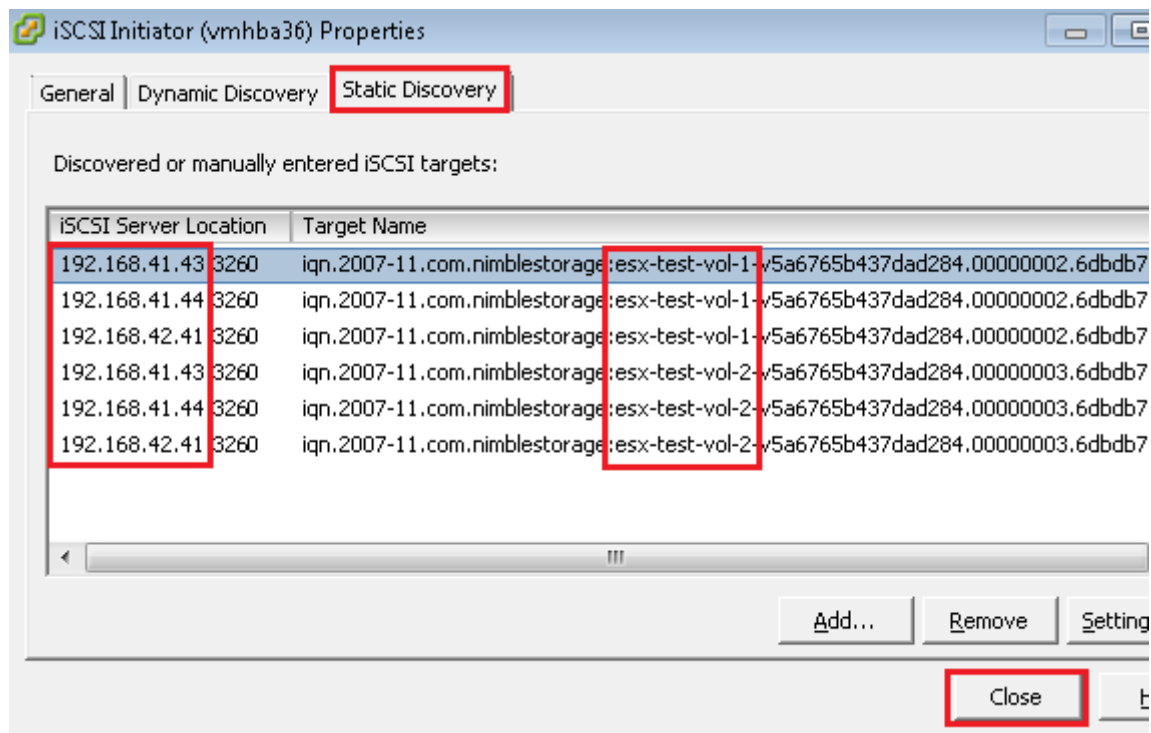
- 4 Verify that the Discovery IP was added correctly.



- 5 Go to the Static Discovery tab, which displays the list of volumes discovered.

This contains a list of all volumes returned during discovery, even though some might not be accessible. This list is built from information returned by the array, not from actual connections.

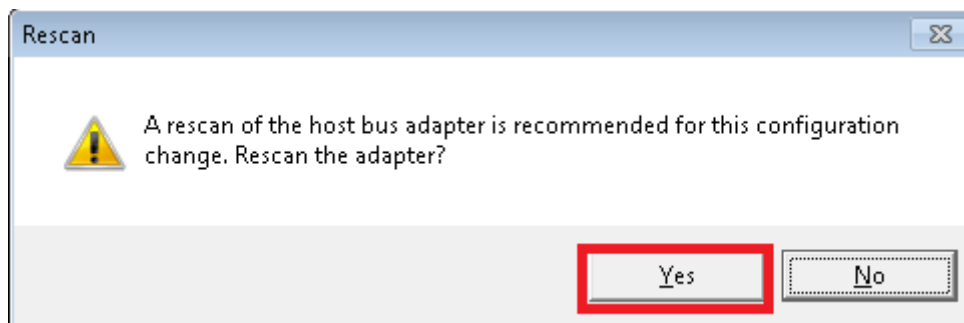
In this example, even though 192.168.42.41 is defined as a Data IP on a Nimble array, the IP is on a different subnet, therefore the ESXi host cannot connect to any volumes on the array.



To continue, click **Close**.

A dialog box appears prompting you to rescan the adapter.

- 6 Click **Yes**.



The device list is updated with any new devices.

7 Click **Paths** and sort the list by the Target column.

In this example, two new devices, corresponding to the two newly discovered volumes, are now listed.

es Resource Allocation Performance Configuration Local Users & Groups

Storage Adapters

Device	Type	WWN
iSCSI Software Adapter		
vmhba36	iSCSI	iqn.1998-01.com.v...
SB700/SB800 IDE Controller		
vmhba1	Block SCSI	
vmhba35	Block SCSI	
SB700 SATA Controller [IDE Mode]		
vmhba0	Block SCSI	

Details

vmhba36

Model: iSCSI Software Adapter
 iSCSI Name: iqn.1998-01.com.vmware:suppvm01-791a0db0
 iSCSI Alias:
 Connected Targets: 8 Devices: 2 Paths: 8

View: Devices **Paths**

Name	Runtime Name	LUN	Type
Nimble iSCSI Disk (eui.e7a577ac4c...)	vmhba36:C0:T1:L0	0	disk
Nimble iSCSI Disk (eui.162d40846a...)	vmhba36:C0:T0:L0	0	disk

The Paths view lists all the actual paths ESXi has to each volume. The Runtime Name contains four items for each path:

- vmhba## – Stays the same across all the iSCSI software adapter entries.
- C# – For each volume, the channel number starts at C0 and increments for each path found to that volume.
- T# – Each volume has its own Target number. It identifies a known volume between this Paths view and the Device view.
- L# – The LUN number is always be zero for Nimble volumes.

For newly discovered devices, only one path is used for I/O by default.

es Resource Allocation Performance Configuration Local Users & Groups Events Permissions

Storage Adapters

Device	Type	WWN
iSCSI Software Adapter		
vmhba36	iSCSI	iqn.1998-01.com.vmware:suppvm01-791a0db0:
SB700/SB800 IDE Controller		
vmhba1	Block SCSI	
vmhba35	Block SCSI	
SB700 SATA Controller [IDE Mode]		
vmhba0	Block SCSI	

Details

vmhba36

Model: iSCSI Software Adapter
 iSCSI Name: iqn.1998-01.com.vmware:suppvm01-791a0db0
 iSCSI Alias:
 Connected Targets: 8 Devices: 2 Paths: 8

View: **Devices** **Paths**

Runtime Name	Target	LUN	Status
vmhba36:C1:T0:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-1-v5a6765b...	0	Active (I/O)
vmhba36:C0:T0:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-1-v5a6765b...	0	Active
vmhba36:C3:T0:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-1-v5a6765b...	0	Active
vmhba36:C2:T0:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-1-v5a6765b...	0	Active
vmhba36:C1:T1:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-2-v5a6765b...	0	Active (I/O)
vmhba36:C0:T1:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-2-v5a6765b...	0	Active
vmhba36:C3:T1:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-2-v5a6765b...	0	Active
vmhba36:C2:T1:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-2-v5a6765b...	0	Active

8 Click the **Devices** tab to continue.

Storage Adapters Refresh

Device	Type	WWN
iSCSI Software Adapter		
vmhba36	iSCSI	iqn.1998-01.com.vmware:suppvm01-791a0db0:
SB700/SB800 IDE Controller		
vmhba1	Block SCSI	
vmhba35	Block SCSI	
SB700 SATA Controller [IDE Mode]		
vmhba0	Block SCSI	

Details

vmhba36

Model: iSCSI Software Adapter
 iSCSI Name: iqn.1998-01.com.vmware:suppvm01-791a0db0
 iSCSI Alias:
 Connected Targets: 8 Devices: 2 Paths: 8

View: **Devices** **Paths**

Name	Runtime Name	LUN	Type	Transport	Capacity	Owner	Hardware
Nimble iSCSI Disk (eui.162940846a...	vmhba36:C0:T0:L0	0	disk	iSCSI	500.00 G	NMP	Unknown
Nimble iSCSI Disk (eui.e7a577ac4c...	vmhba36:C0:T1:L0	0	disk	iSCSI			Unknown

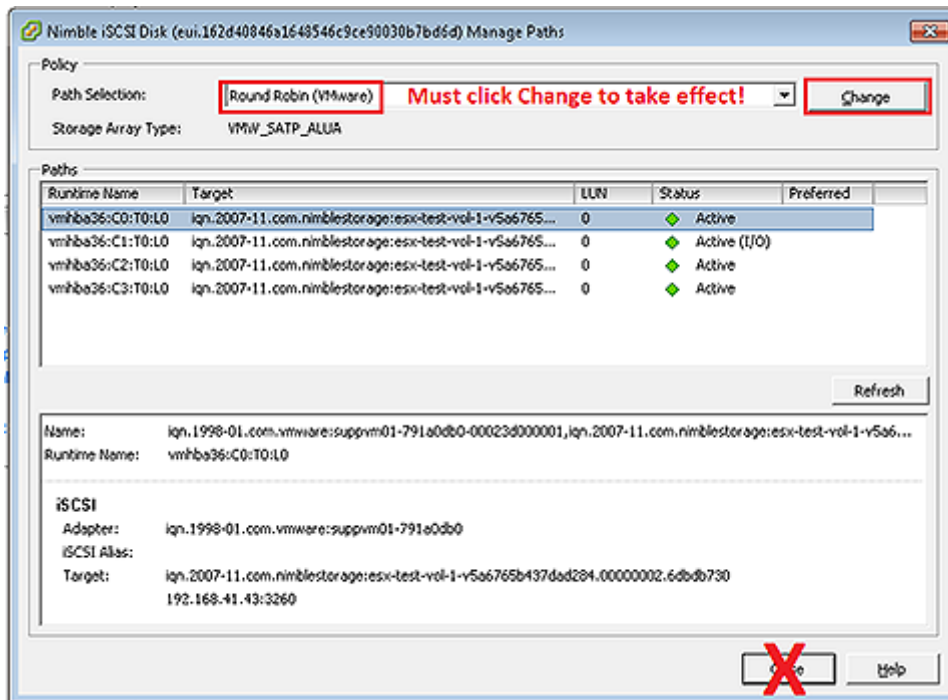
Rename
Manage Paths...
 Copy identifier to clipboard

The Devices view lists each device to which ESXi has connections. Each Nimble volume is shown as one device. Use the Target number of the Nimble volume to locate its device entry in Device view.

9 Select the T0 entry, right-click and select **Manage Paths**.

10 Change the Path Selection policy to "Round Robin (VMware)" and click **Change**.

Note You must click **Change** for the Path Selection policy to take effect. Do NOT click **Close**.



11 Ensure that the status of all paths changes to "Active (I/O)." Then click **Close**.

Active (I/O) indicates Round Robin is now in effect, and all paths can be used for I/O.

iSCSI Disk (eui.162d40846a1648546c9ce90030b7bd6d) Manage Paths

Selection: Round Robin (VMware)

Array Type: VMW_SATP_ALUA

Name	Target	LUN	Status	Preferred
h:C0:T0:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-1-v5a6765...	0	Active (I/O)	
h:C1:T0:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-1-v5a6765...	0	Active (I/O)	
h:C2:T0:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-1-v5a6765...	0	Active (I/O)	
h:C3:T0:L0	iqn.2007-11.com.nimblestorage:esx-test-vol-1-v5a6765...	0	Active (I/O)	

Name: vmhba36:C0:T0:L0

Target: iqn.1998-01.com.vmware:suppvm01-791a0db0-00023d000001,iqn.2007-11.com.nimblestorage:esx-test-vol-1-v5a6765b437dad284.00000002.6dbdb730

IP: 192.168.41.43:3260

Close


- 12 As needed, repeat the two previous steps to change the path selection policy on the ESXi host for the other Nimble devices/volumes.

iSCSI Host Connection Methods

The iSCSI initiators on the host connect with targets on the array through the data ports on each controller. Each port is identified by its IP address.

Beginning with the NimbleOS 2.0 release, the default iSCSI host connection management method is *Automatic*. When you install the Nimble Connection Service (NCS) on your Windows or VMware hosts, the process of adding target portals and connecting volumes to iSCSI targets is also simplified.

Each subnet, management or data, has a unique discovery IP address.

Figure 3: Discovery IP in the NimbleOS GUI


Subnet Label	Network	Netmask	Traffic Type	Traffic Assignment	Discovery IP	IP Address Zone	MTU	Bytes	VLAN ...
data1	198.51.100.0	255.255.255.0	Data only	iSCSI + Group	198.51.100.55	Single	Standard	1500	
mgmt-data	192.0.2.0	255.255.255.0	Mgmt only		192.0.2.51		Standard	1500	

Important The discovery IP address must be accessible by at least one host initiator port.

Automatic iSCSI Host Connections

The Automatic iSCSI connection method uses data subnet discovery IPs for host connection. The Nimble array then automatically redirects the connection to an appropriate iSCSI data IP. The Automatic method is the better choice for most applications.

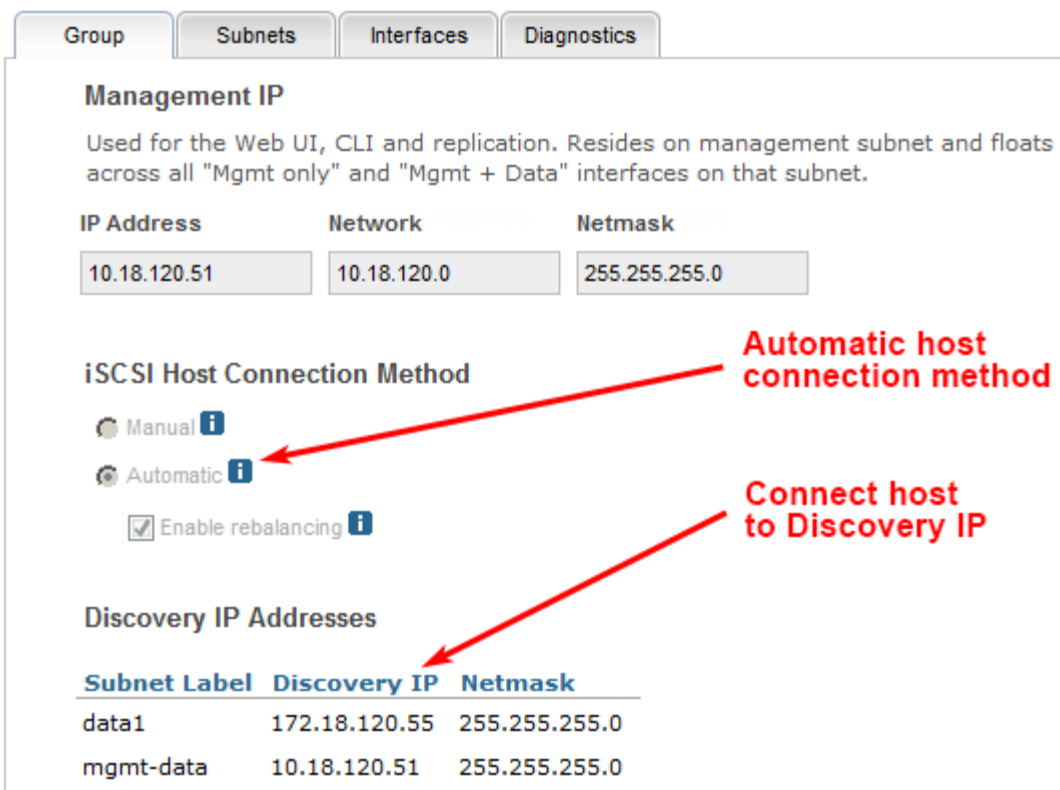


Go to **Administration > Network Configuration** and click **Active Settings**.

On the array, when the iSCSI host connection method is set to Automatic:

[Network Configurations](#)

[View](#)





Management IP


Used for the Web UI, CLI and replication. Resides on management subnet and floats across all "Mgmt only" and "Mgmt + Data" interfaces on that subnet.

IP Address	Network	Netmask
10.18.120.51	10.18.120.0	255.255.255.0

iSCSI Host Connection Method

☐ Manual 

☒ Automatic 

☒ Enable rebalancing 

Discovery IP Addresses

Subnet Label	Discovery IP	Netmask
data1	172.18.120.55	255.255.255.0
mgmt-data	10.18.120.51	255.255.255.0



At the command prompt, type **netconfig --info active**.


```
Nimble OS $ netconfig --info active
Group Management IP: 10.18.120.51/255.255.255.0
Group leader array: c20-array2
Member array(s): c20-array2
ISCSI Automatic connection method: Yes
ISCSI Connection rebalancing      : Yes
```

**Automatic host
connection method**

Routes:

Destination	Netmask	Gateway
0.0.0.0	0.0.0.0	10.18.120.1

**Connect Host
to Discovery IP**

Subnets:

Label	Network	Type	Discovery IP	VLAN	MTU
data1	172.18.120.0/24	Data	172.18.120.55	0	1500
mgmt-data	10.18.120.0/24	Mgmt	10.18.120.51	0	1500

Array Network Configuration: c20-array2

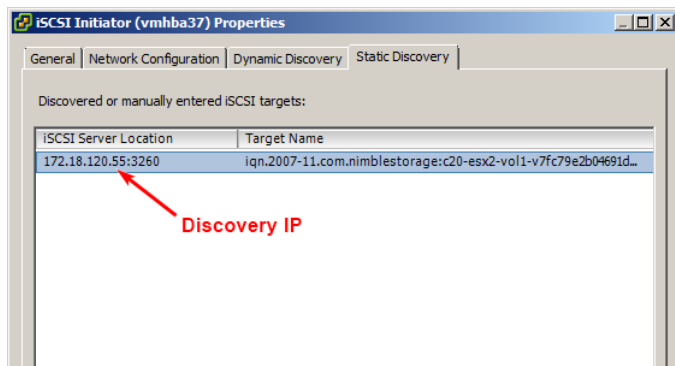
Controller A IP: 10.18.120.54

Controller B IP: 10.18.120.55

NIC	Subnet Label	Data IP Address	Tagged
eth1	mgmt-data	N/A	No
eth2	mgmt-data	N/A	No
eth3	data1	172.18.120.56	No
eth4	data1	172.18.120.57	No
eth5	data1	172.18.120.58	No
eth6	data1	172.18.120.59	No

Nimble OS \$ █

Use a data subnet discovery IP to connect from the host to the array. In the GUI, discovery IPs are listed on the Group and Subnets tabs.



Note The iSCSI host to array connection process is faster and simpler when you install and use Nimble Connection Manager (NCM) on your Windows or VMware host.

See the *Nimble Storage Windows Integration Guide*.

Manual iSCSI Host Connections

NimbleOS v1.4 and earlier releases, hosts connect manually to iSCSI data or discovery IPs. The same is true for NimbleOS v2.0 when the iSCSI connection method is set to *Manual*. The Manual method is intended primarily for legacy applications.



Go to **Administration > Network Configuration** and click **Modify**.

On the array, when the iSCSI host connection method is set to Manual:

[Network Configurations](#)

| [View](#)

Group

Subnets

Interfaces

Diagnostics

Management IP

Used for the Web UI, CLI and replication. Resides on management subnet and floats across all "Mgmt only" and "Mgmt + Data" interfaces on that subnet.

IP Address	Network	Netmask
10.18.120.51	10.18.120.0	255.255.255.0

iSCSI Host Connection Method

☒ Manual i

☐ Automatic i

☐ Enable rebalancing i

Discovery IP Addresses

Subnet Label	Discovery IP	Netmask
data1	172.18.120.55	255.255.255.0
mgmt-data	10.18.120.51	255.255.255.0

Manual host connection method

Discovery IP



At the command prompt, type **netconfig --info active**.

```
Nimble OS $ netconfig --info active
Group Management IP: 10.18.120.51/255.255.255.0
Group leader array: c20-array2
Member array(s): c20-array2
ISCSI Automatic connection method: No
ISCSI Connection rebalancing      : No
```

**Manual host
connection method**



Routes:

Destination	Netmask	Gateway
0.0.0.0	0.0.0.0	10.18.120.1

**Connect Host
to Discovery IP**



Subnets:

Label	Network	Type	Discovery IP	VLAN	MTU
data1	172.18.120.0/24	Data	172.18.120.55	0	1500
mgmt-data	10.18.120.0/24	Mgmt	10.18.120.51	0	1500

Array Network Configuration: c20-array2

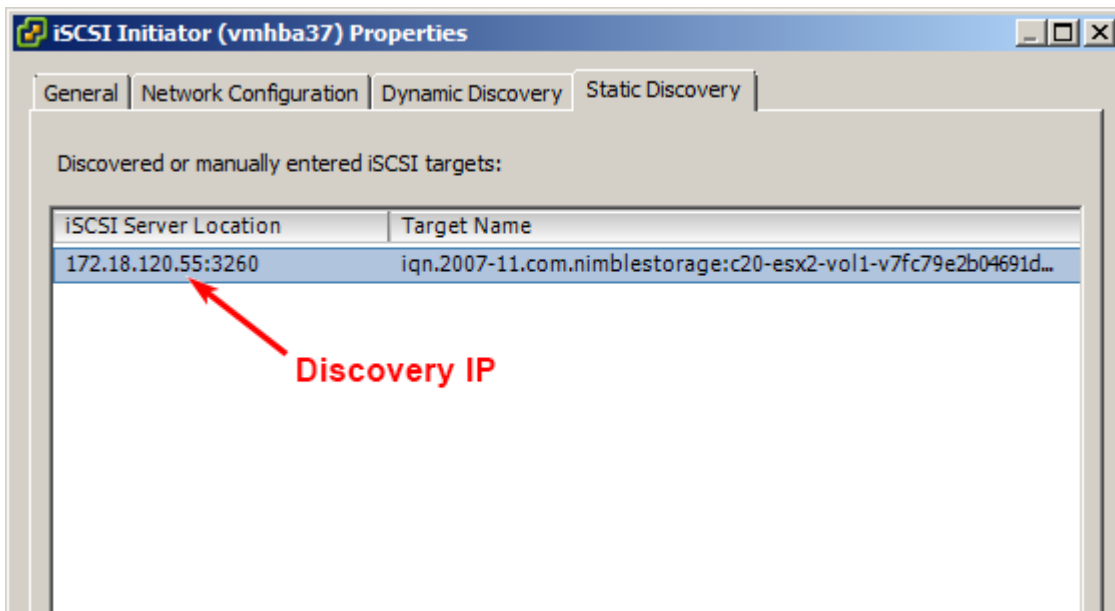
Controller A IP: 10.18.120.54

Controller B IP: 10.18.120.55

NIC	Subnet Label	Data IP Address	Tagged
eth1	mgmt-data	N/A	No
eth2	mgmt-data	N/A	No
eth3	data1	172.18.120.56	No
eth4	data1	172.18.120.57	No
eth5	data1	172.18.120.58	No
eth6	data1	172.18.120.59	No

Nimble OS \$ █

Use a data subnet discovery IP to connect from the VMware host to the array. In the GUI, discovery IPs are listed on the Group and Subnets tabs.



Set the iSCSI Host Connection Method to Manual

The manual iSCSI host connection method is intended primarily so that you can configure legacy applications to use the automatic connection method after upgrading to Nimble OS 2.0 or later. (Neither option applies to Fibre Channel arrays.)

Procedure

- 1 Disable automatic rebalancing of the iSCSI host connections.
netconfig --edit active --iscsi_connection_rebalancing no
- 2 Disable automatic iSCSI host connections.
netconfig --edit active --iscsi_automatic_connection_method no

Example

Example:

```
Nimble OS $ netconfig --edit active --iscsi_connection_rebalancing no
Nimble OS $ netconfig --edit active --iscsi_automatic_connection_method
no
```

Configure Jumbo Frames

Note This section is optional. If you do not need to enable Jumbo Frames, skip this section and go to [Configure iSCSI Discovery](#) on page 113.

If you configure your environment for Jumbo Frames, every device in the network path must be set up for Jumbo Frames. Depending on your network infrastructure, that includes but is not limited to:

- Physical network switches
- Nimble arrays
- ESX vSwitches

- ESX vmk ports

To set Jumbo Frames on the Nimble array, go to [Change NIC Frame Size](#) on page 127. To set Jumbo Frames on your physical network switches, refer to the vendor documentation.

Caution When setting Jumbo Frames in ESX, change vSwitches first. Then immediately change the vmk ports.

If you do not change the vmk ports immediately after the vSwitches, unexpected path behavior can occur, such as the paths going up and down.

This task must be done from a console session to the ESX host, such as an SSH session (Remote Tech Support session) to the host.

Procedure

To enable Jumbo Frames for ESX vSwitches and vmk ports:

- 1 Establish an SSH session to the host and log in as root.
- 2 View a list your vSwitches. Type:

esxcfg-vswitch --list

Note the name of the vSwitch(es) created earlier that you want to enable Jumbo Frames on. Verify the switch name(s) by ensuring that the vmnic uplinks and port group names are the correct ones. In this example, the switch is *vSwitch1*.

```

192.168.43.11 - PuTTY
~ # esxcfg-vswitch --list
Switch Name      Num Ports   Used Ports   MTU      Uplinks
vSwitch0         128         3            1500     vmnic0

  PortGroup Name  VLAN ID    Used Ports
  VM Network      0          0
  Management Network 0          1

Switch Name      Num Ports   Used Ports   MTU      Uplinks
vSwitch1         128         5            1500     vmnic2,vmnic3

  PortGroup Name  VLAN ID    Used Ports
  iSCSI2          0          1
  iSCSI1          0          1
~ #

```

- 3 For each vSwitch, type:

esxcfg-vswitch --mtu=9000 <vswitch##>

Where <vswitch##> is the name of the vSwitch on which you want to enable jumbo frames.

```

192.168.43.11 - PuTTY
~ # esxcfg-vswitch --mtu=9000 vSwitch1
~ #

```

- 4 Verify that the vSwitch(es) have Jumbo Frames enabled. Type:

esxcfg-vswitch --list

```

192.168.43.11 - PuTTY
~ # esxcfg-vswitch --list
Switch Name      Num Ports   Used Ports   Configured Ports   MTU      \
vSwitch0         128         3            128               1500     \

  PortGroup Name   VLAN ID   Used Ports   Uplinks
  VM Network       0         0            vmnic0
  Management Network 0         1            vmnic0

Switch Name      Num Ports   Used Ports   Configured Ports   MTU      \
vSwitch1         128         5            128               9000     \

  PortGroup Name   VLAN ID   Used Ports   Uplinks
  iSCSI2           0         1            vmnic3
  iSCSI1           0         1            vmnic2

~ #

```

Continue with the remaining steps to immediately modify the vmk ports.

- 5 List the vmk ports created earlier and their port group names. Type:

esxcfg-vmknic --list

In this example, the names are *iSCSI1* and *iSCSI2*.

```

192.168.43.11 - PuTTY
~ # esxcfg-vmknic --list
Interface  Port Group/DVPort  IP Family  IP Address  MAC Address  MTU  TSO MSS  Enabled  Type
vmk0       Management Network IPv4        192.168.43.125 00:25:90:23:46:0c 1500 65535    true    STATIC
vmk1       iSCSI1             IPv4        192.168.41.11  00:50:56:7a:ba:d2 1500 65535    true    STATIC
vmk2       iSCSI2             IPv4        192.168.41.111 00:50:56:79:d3:b9 1500 65535    true    STATIC

~ #

```

- 6 Enable Jumbo Frames on a port group. Type:

esxcfg-vmknic --mtu 9000 <pg_name>

Where <pg_name> is the port group name (not the vmk name) of the vmk/port group.

```

192.168.43.11 - PuTTY
~ # esxcfg-vmknic --mtu 9000 iSCSI1
~ # esxcfg-vmknic --mtu 9000 iSCSI2
~ #

```

- 7 Verify that the vmks/port groups have Jumbo Frames enabled. Type:

esxcfg-vmknic --list

```

192.168.43.11 - PuTTY
~ # esxcfg-vmknics --list
Interface  Port Group/VNPort  IP Family  IP Address  MAC Address  MTU  TSO MSS  Enabled  Type
vmk0      Management Network  IPv4       192.168.3.255  00:25:90:23:46:0c  1500  65535   true    STATIC
vmk1      iSCSI1             IPv4       192.168.41.111  08:50:56:7a:ba:d2  9000  65535   true    STATIC
vmk2      iSCSI2             IPv4       192.168.41.111  28:56:79:d3:b9    9000  65535   true    STATIC
~ #

```

Change NIC Frame Size

This procedure sets the frame size for each NIC on your array. Do not select Jumbo Frames unless all of your network components support them.

Procedure

- 1 At the command prompt, type **nic --edit <nicname> --mtu <number>**
For **<number>**, use 1500 for "standard," 9000 for "jumbo," or type a custom number.
- 2 View a list of all NICs by typing **nic --list**.

Change NIC Frame Size

This procedure sets the frame size for each NIC on your array. Do not select Jumbo Frames unless all of your network components support them.

Procedure

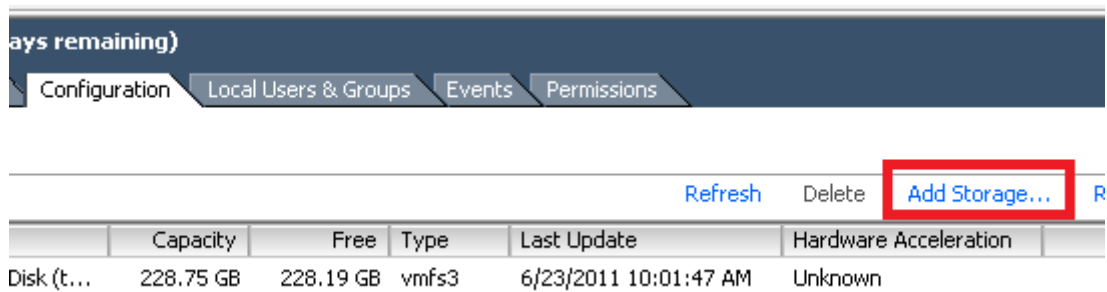
- 1 From the dashboard, choose **Admin > Network**.
- 2 Click **Configure Active Settings**.
- 3 Click the **Subnets** tab.
- 4 Click **Edit**.
- 5 Check the checkbox next to the subnet that you want to modify and click **Edit**.
The MTU settings are in the top section of the page.
- 6 Choose the frame size from the MTU dropdown menus.
If you select Other, you must also include the number of bytes to use for the frame size.
- 7 Click **Done**.

Configure an ESX Datastore

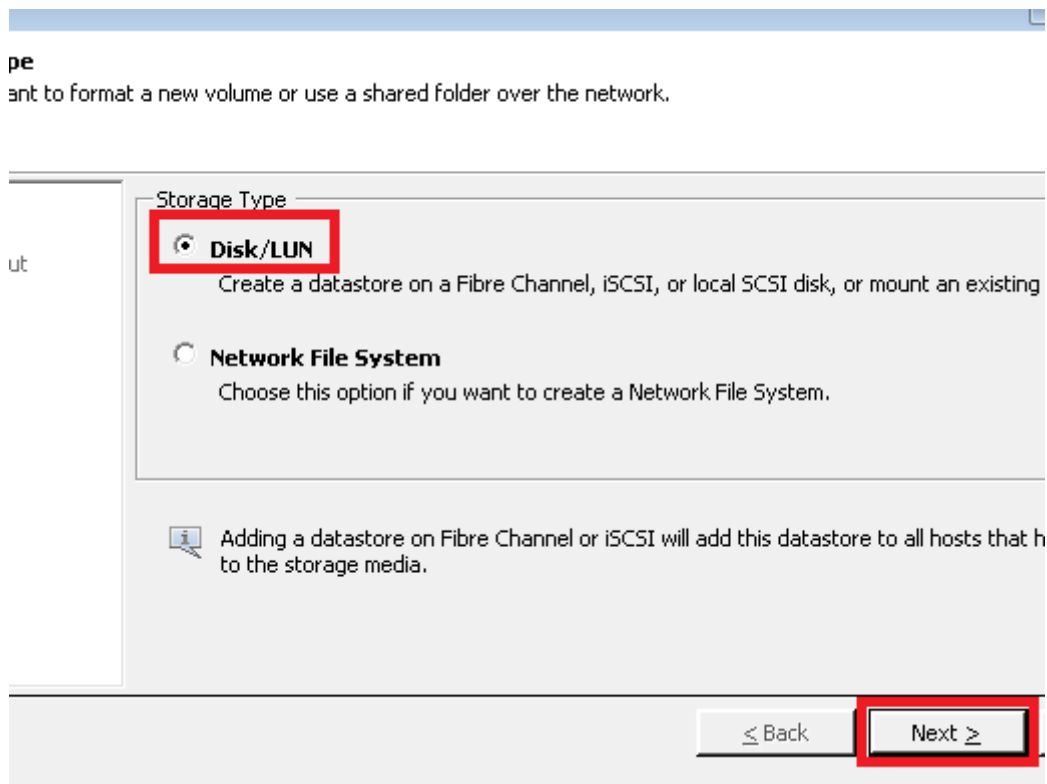
Procedure

To create a datastore from a newly presented Nimble volume:

- 1 Go to the Configuration / Storage screen on the ESX host and click **Add Storage**.
In this example, the only existing datastore is a local ATA disk in the host itself.



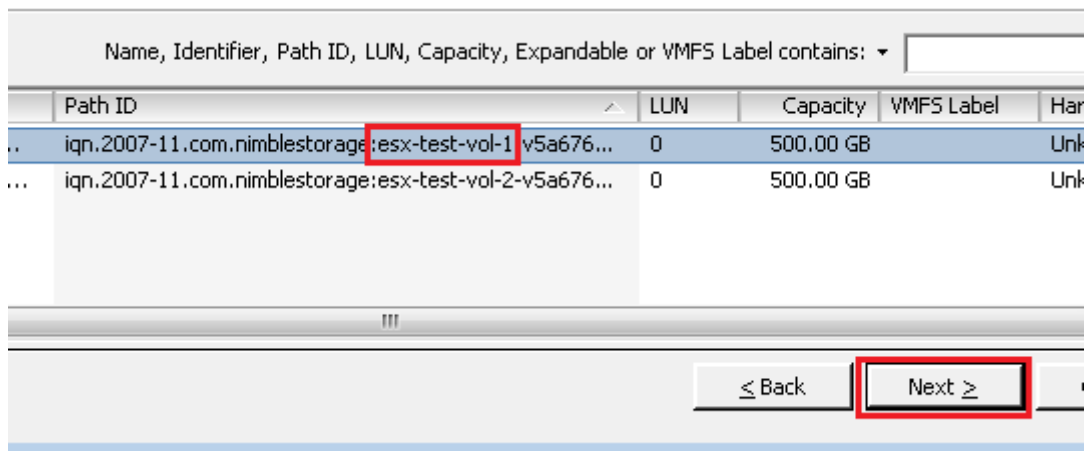
- 2 Under Storage Type, choose the Disk/LUN option and click **Next**.



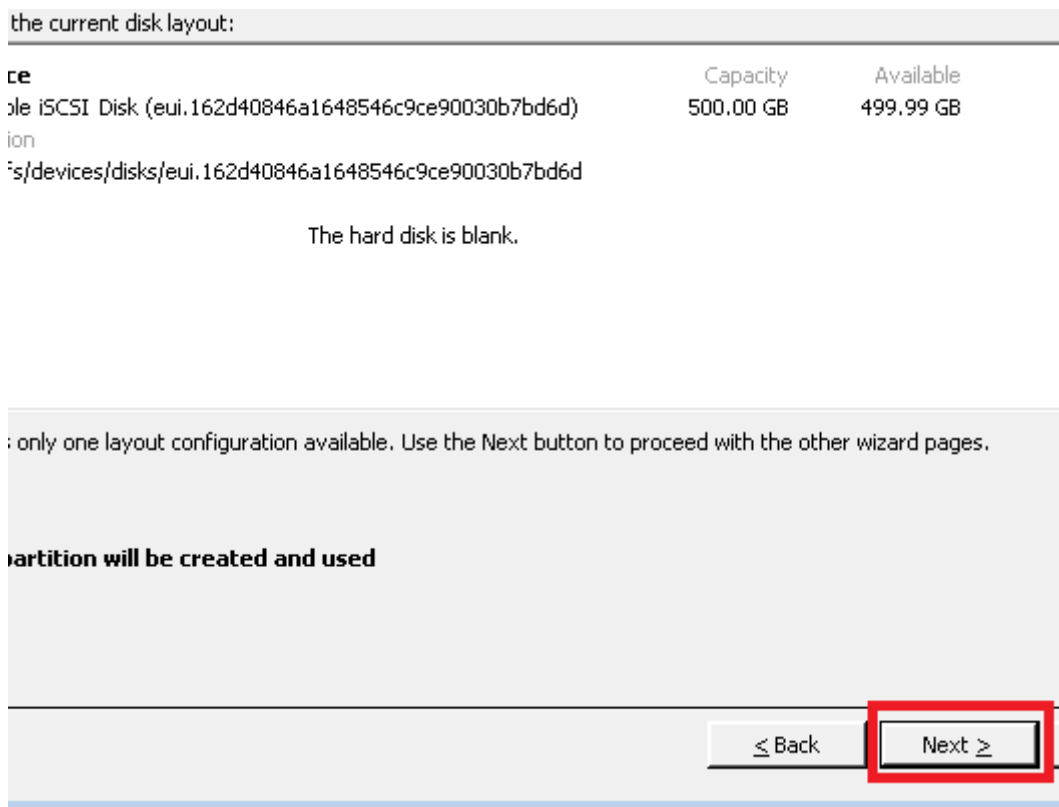
Volumes that are eligible to become datastores are listed.

Expand the Path ID column until you can see the entire volume name.

- 3 Select the appropriate volume and click **Next**.
In this example, the volume is *esx-test-vol-1*.



- 4 Review the proposed configuration and click **Next**.



- 5 Enter a datastore name and click **Next**.
In this example, the name is *Datastore-temp-1*.

Add Storage

Properties
Specify the properties for the datastore

Disk/LUN
[Select Disk/LUN](#)
[Current Disk Layout](#)
Properties

Enter a datastore name
Datastore-temp-1

Help ≤ Back **Next >** Cancel

- 6 Note the Maximum file size setting. If you need to store files or a VMDK on the datastore larger than the default file size of 256 GB, choose a larger block size.

Max. File Size	Block Size
256 GB	1 MB
512 GB	2 MB
1 TB	4 MB
2 TB	8 MB

Add Storage

Disk/LUN - Formatting
Specify the maximum file size and capacity of the datastore

Maximum file size
Large files require large block size. The minimum disk space used by any file is equal to the file system block size.

256 GB , Block size: 1 MB

Capacity
☒ Maximize capacity 499.99

≤ Back **Next >**

- 7 Check the Maximize capacity box to use the entire volume as the datastore. Click **Next**.
- 8 Review the configuration, then click **Finish**.

File system:

Properties
Datastore name: Datastore-temp-1

Formatting
File system: VMFS-3
Block size: 1 MB
Maximum file size: 256 GB

≤ Back
Finish
Cancel

The datastore is created and the Configuration / Storage screen shows the new datastore.

Summary
Virtual Machines
Resource Allocation
Performance
Configuration
Log

Status
Datastores
Virtual Machines
Adapters
Adapters
Advanced Settings
Management
Features

View: Datastores Devices

Datastores

Identification	Device	Capacity
datastore1	Local ATA Disk (...)	228.75 GB
Datastore-temp-1	Nimble iSCSI Di...	499.75 GB

Datastore Details

Datastore-temp-1

Location: /vmfs/volumes/4e046a8b-1...

- Repeat this procedure to make additional volumes into datastores.

Set the Path Selection Policy to Round Robin (ESXi 5.0, 5.1, 5.5, and 6.0)

This procedure applies to ESXi 5.0, 5.1, 5.5, and 6.0. Nimble Connection Manager (NCM) automatically creates the optimal number of iSCSI sessions for each Nimble volume and manages the selection of paths to the volumes. If you have installed NCM, you do not need to perform this procedure.

This procedure must be done from a console session to the ESXi host, such as an SSH session (Remote Tech Support session) to the host.

Procedure

To set the default to Round Robin for all new Nimble volumes:

- 1 At the command prompt, on a single line, type:
esxcli storage nmp satp rule add --psp=VMW_PSP_RR --satp=VMW_SATP_ALUA --vendor=Nimble
 All newly presented Nimble volumes default to Round Robin.
 All existing volumes retain their old path selection policies.
- 2 Verify the rule was by typing:
esxcli storage nmp satp rule list | grep Nimble
- 3 Change all existing Nimble volumes to Round Robin by running the following script:
**for i in `esxcli storage nmp device list | egrep [add a space here]
 "^euil\w{16}(6c9ce9|6C9CE9)\w{10}"` ; do esxcli [add a space here]
 storage nmp device set --device \$i --psp=VMW_PSP_RR ; done**
Caution
 This script must be typed on a single line EACTLY as shown.
 If possible, copy each line of the script from this page and paste it directly into the command line.
- 4 For all existing Nimble volumes and every new added Nimble volume, type the following command to change the policy type to iops and set iops option to one :
esxcli storage nmp psp roundrobin deviceconfig set --type=iops --iops=1 -d <devicename>

Enable Application-Consistent Quiescing on Windows Server 2008 VM

This procedure applies to Windows Server 2008 virtual machines (VMs) that were created on an ESX/ESXi 4.0 host and later migrated to a newer host, such as an ESXi 5.0, 5.1, 5.5, or 6.0 host.

Windows Server 2008 virtual machines (VMs) created on an ESX/ESXi 4.0 host and migrated to a newer host are not enabled for application-consistent quiescing. Those VMs require the configuration parameter *disk.EnableUUID = TRUE*. In the absence of this parameter, vCenter-synchronized backups complete successfully and give the impression that they are application consistent. In this case however, the backups do not have application-consistent snapshots. Such snapshots are not supported by Microsoft Exchange or SQL in their restore scenarios.

Procedure

To enable the *disk.EnableUUID = TRUE* parameter:

- 1 Start the vSphere Client, and log in to a vCenter Server.
- 2 Select Virtual Machines and Templates and click the Virtual Machines tab.
- 3 Right-click the Windows 2008 VM for which you are enabling the disk UUID parameter, and select **Power > Power Off**.
 The VM powers off.
- 4 Right-click the VM, and click **Edit Settings**.
- 5 Click the Options tab, and select the General entry in the settings column.
- 6 Click **Configuration Parameters....**
 The Configuration Parameters window appears.
- 7 Click **Add Row**.
- 8 In the Name column, type:
disk.EnableUUID
- 9 In the Value column, type:
TRUE

10 Click **OK** and then click **Save**.

11 Power on the VM.

Results

With the UUID parameter added, application-consistent quiescing is enabled for the Windows Server 2008 VM that was created on an ESX/ESXi 4.0 host and later migrated to a newer host.

Log in to the NimbleOS CLI

This procedure creates a CLI connection over your network. To create a CLI connection through the serial port on the array, see [Set up a Serial Connection](#) on page 134.

Before you begin

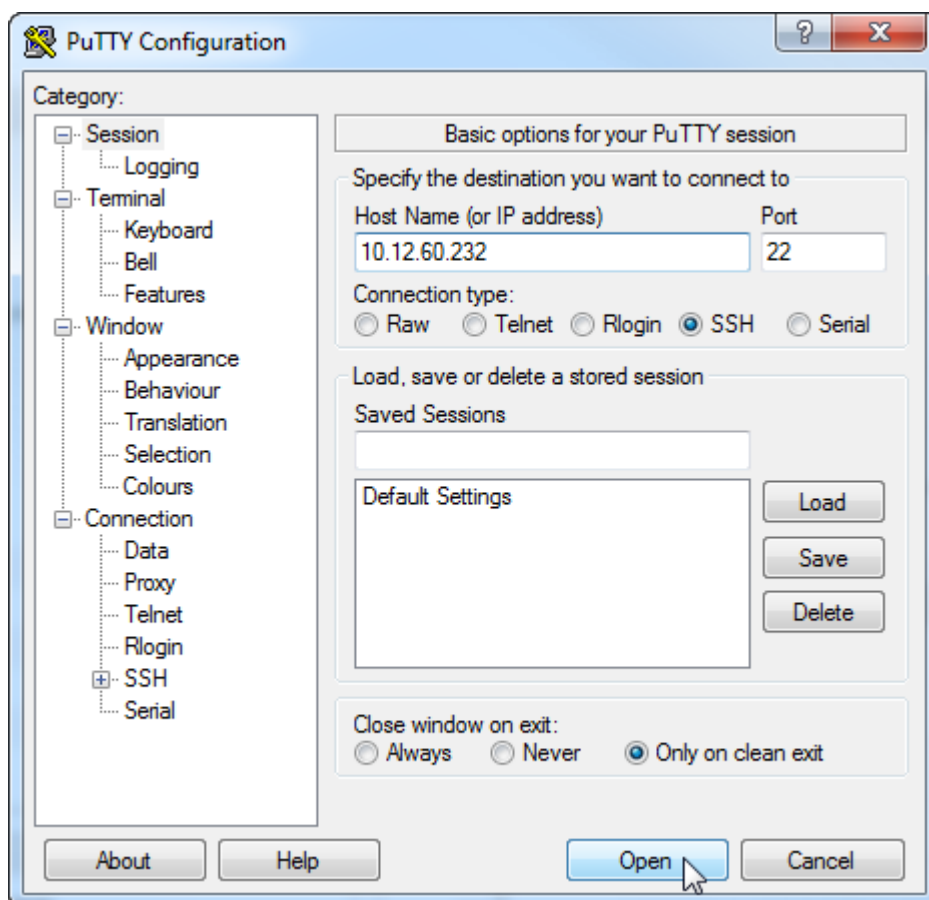
To complete this task, you need:

- The array IP address
- The array login ID and password
- An SSH client on the Windows server, such as PuTTY

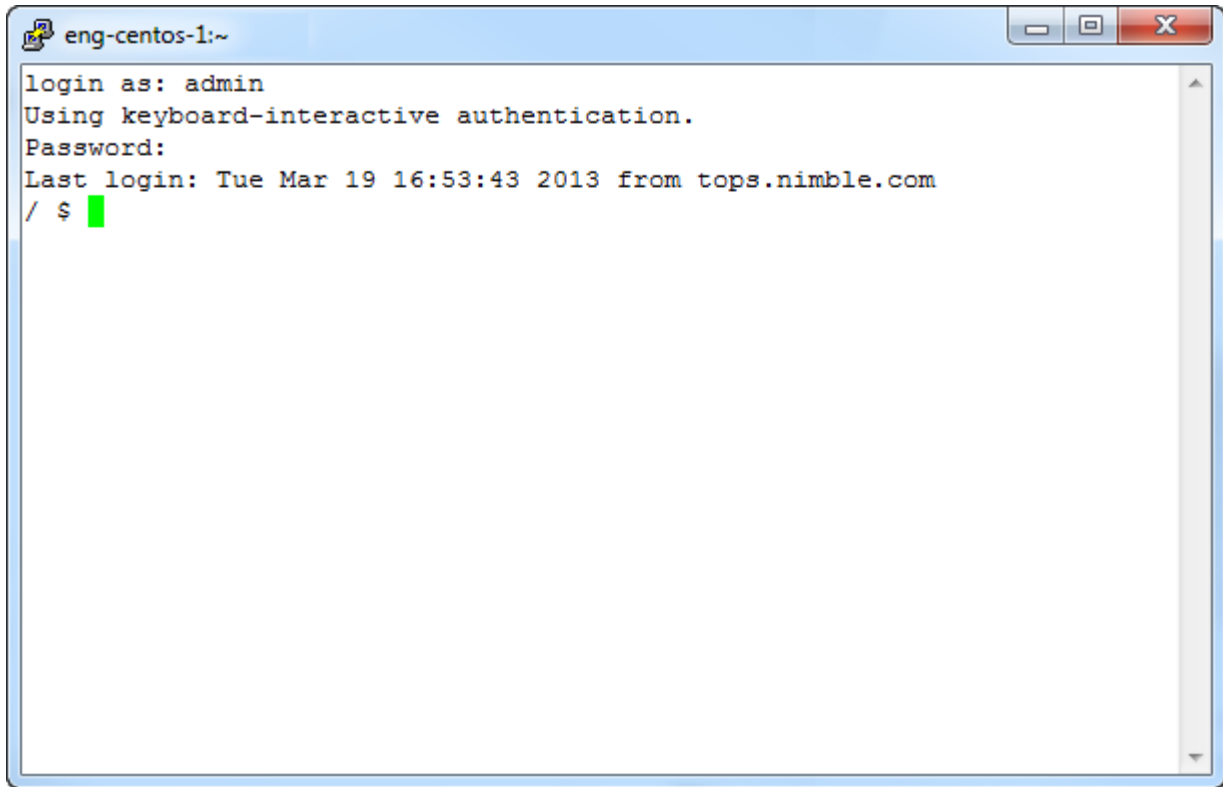
Procedure

To log into the NimbleOS CLI:

- 1 Open your SSH client.
- 2 Type the IP address of the array and click **Open**.



- 3 In the CLI, type the user name and press Enter.



- 4 Type the password and press Enter.
When the command prompt returns, the array is ready to accept commands.

Set up a Serial Connection

The CLI requires a serial connection for the initial setup of the array. After setup, the CLI can also use an SSH connection over the network.

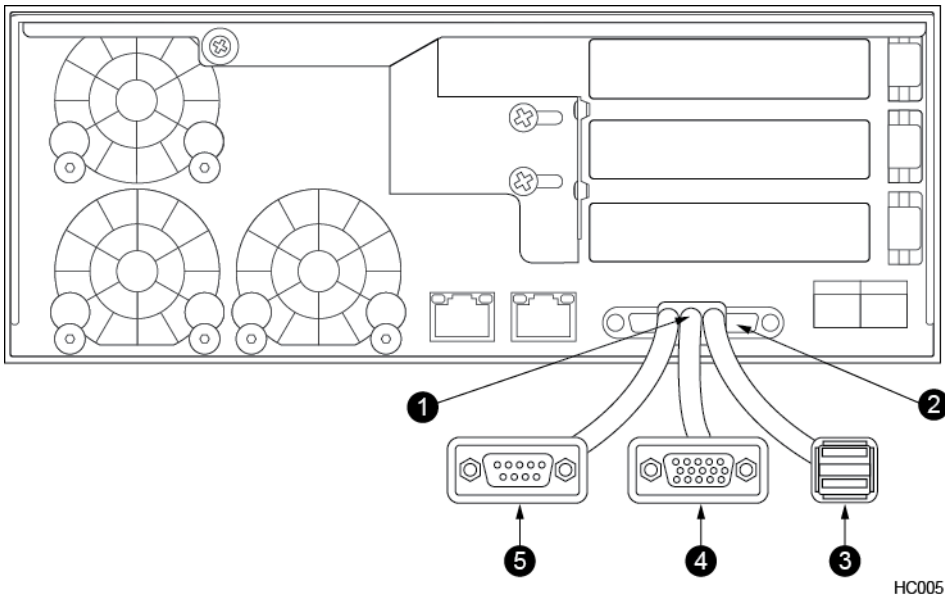
Before you begin

Obtain these items:

- Laptop computer or workstation
- Null-modem cable with DB9-female connector at one end and the appropriate connector on the other to mate with the serial interface (typically USB) on the laptop computer or workstation
- Serial-USB-VGA adapter (dongle) from the Accessories kit that came with your array

Procedure

- 1 Attach the Serial-USB-VGA adapter (dongle) to the KVM port on Controller A.



- 2 Connect a null-modem cable to the DB9-male connector on the adapter. Connect the other end of the null-modem cable to the serial port on your laptop computer or workstation.
- 3 Run the serial console software with the following settings:

Data bits:	8
Parity:	None
Stop bits:	1
Speed:	115.2Kbps

- 4 Log in as user `admin` with the password `admin`.

Note You can only log into the active controller. If you cannot log in, move the Serial-USB-VGA adapter to the other controller and try to log in again.

After you have logged in, the CLI is ready to accept commands.

What to do next

Type `?` to see a list of commands.

Type the command followed by `--help` to see the usage information for that command.

Set up a Direct Connection

The CLI supports a direct connection for the initial setup of the array. After setup, the CLI can also use an SSH connection over the network.

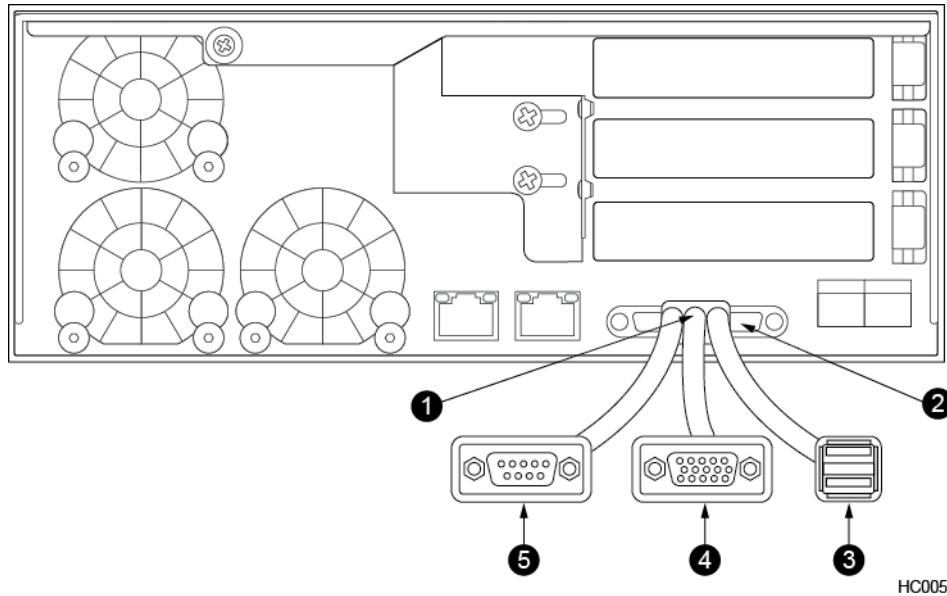
Before you begin

Obtain these items:

- Computer monitor that supports a VGA connection
- Computer keyboard that supports a USB connection
- Serial-USB-VGA adapter (dongle) from the Accessories kit that came with your array

Procedure

- 1 Attach the Serial-USB-VGA adapter (dongle) to the KVM port on Controller A.



- | | |
|--------------------------|--------------------|
| 1 Serial-USB-VGA adapter | 4 VGA connector |
| 2 Controller KVM port | 5 Serial connector |
| 3 USB connector | |

- 2 Connect the video cable from your monitor to the VGA connector on the adapter.
Plug the monitor into a suitable power source.
- 3 Connect the USB cable from your keyboard to the USB connector on the adapter.
- 4 Log in as user `admin` with the password `admin`.

Note You can only log into the active controller. If you cannot log in, move the Serial-USB-VGA adapter to the other controller and try to log in again.

Once you have logged in, the CLI is ready to accept commands.

What to do next

Type `?` to see a list of commands.

Type the command followed by `--help` to see the usage information for that command.

iSCSI Initiator Groups

The Nimble array uses iSCSI initiators and iSCSI targets as a method of communication. iSCSI Initiator groups limit access to Nimble iSCSI target volumes and snapshots (data providers) on the array.

An iSCSI initiator group has three primary functions:

- To allow initiator access to volumes
- To limit (using IP-based ACL) initiator access to volumes

- To deny initiator access to volumes

An iSCSI initiator group consists of one or more client iSCSI initiators on the host system and either all configured subnets or selected target subnets.

Create an iSCSI Initiator Group Using the GUI

In a VMware environment, an iSCSI group enables access for specific clients to specific volumes over specific subnets.

Before you begin

To create an iSCSI initiator group using the VMware vSphere Web Client GUI, you must know the iSCSI Qualified Name (IQN) and IP address of each client. The client might be a Windows host, an ESXi host, or any another computer that needs to access a volume on your Nimble array. Configure your client initiator according to the vendor's recommendations.

Procedure



To create an iSCSI initiator group:

- 1 From the home page, select **Manage > Data Access**.
- 2 On the Initiator Groups page, click **Add** (the plus icon).
- 3 Type an iSCSI initiator group name in the Name field.
- 4 Under **Subnets**, choose one of the following:

- Use all configured subnets
- Use selected subnets

If you choose Use selected subnet, a list of available subnets is displayed.

- a) (Optional) Highlight the subnets you want to associate with this iSCSI initiator group and click **Add**, on

the left side of the dialog box.

- b) Type a name for the initiator in the Name field.
 - c) Copy and paste the IQN of the client system into the IQN field.
- Note** If you cannot copy and paste the IQN, type it very carefully.
- d) Type the IP address of the client system in the IP Address field.
 - a) Click **OK**.

- 5 (Optional) If you want to add another initiator, click **Add**
- 6 If you have added all initiators, click **Create** again.

Create an iSCSI Initiator Group

In a VMware environment, an iSCSI group enables access for specific clients to specific volumes over specific subnets.

Before you begin

To create an iSCSI initiator group, you must know the iSCSI Qualified Name (IQN) and IP address of each client. The client might be a Windows host, an ESXi host, or any another computer that needs to access a volume on your Nimble array. Configure your client initiator according to the vendor's recommendations.

Procedure

- 1 At the command prompt, type:

```
initiatorgrp --create <initiator group name>
```

Example: **initiatorgrp -- create Dataman**

- 2 Type the following command to add an initiator:

```
initiatorgrp --add_initiators <initiator group name> --label <initiator label> [--initiator_name <IQN> | --ipaddr <client system IP address>]
```

Example: **initiatorgrp --add_initiators Dataman --label client1 --initiator_name iqn.1991-05.com.microsoft:techops.storage.com --ipaddr 192.0.2.88**

Note If you cannot copy-and-paste the IQN, type it very carefully.

- 3 Type the following command to add a subnet:

```
initiatorgrp --add_subnets <initiator group name> --label <subnet label>
```

Example: **initiatorgrp --add_subnets Dataman --label Subnet-198.51.100.0**

- 4 Type the following command to verify your iSCSI initiator group:

```
initiatorgrp --info <initiator groupname>
```

Example: **initiatorgrp --info Dataman**

You should see a result like this:

```
Name: Dataman
Description:
Access Protocol: iscsi
Created: Feb 19 2014 16:16:32
Last configuration change: Feb 19 2014 16:16:32
Number of Subnets: 1
    Subnet Label: Subnet-198.51.100.0
Number of Initiators: 1
    Initiator Label: Basic
        Initiator Name: iqn.1991-05.com.microsoft:techops.storage.com
        Initiator IP Address: 198.0.2.88
```

Example

```
initiatorgrp -- create Dataman
initiatorgrp --add_initiators Dataman --label client1 --initiator_name
iqn.1991-05.com.microsoft:techops.storage.com --ipaddr 192.0.2.88
```

```
initiatorgrp --add_subnets Dataman --label Subnet-198.51.100.0
initiatorgrp --info Dataman
```

Assign Volumes to an iSCSI Initiator Group Using the GUI

You can assign an existing volume to an iSCSI initiator group using the VMware vSphere Web Client GUI. You can also assign a volume to an iSCSI initiator group when you create the volume.

See "Create a Volume Using the GUI" or "Create a Volume Using the CLI" in the *Nimble Storage Installation Guide*.

Before you begin

You must create your iSCSI initiator groups before you can assign volumes to them.

Procedure

To assign a volume to an iSCSI initiator group in the GUI:

- 1 From the dashboard, go to **Manage > Data Storage**.
- 2 On the Volumes page, check the volume you want to assign to the iSCSI initiator group.
- 3 Click **Edit** (the pencil icon).
- 4 Click Access on the progress bar.
- 5 Click **Add**.
- 6 In the Add ACL dialog box, choose whether you want to limit access to:
 - The volume and its snapshots
 - The volume only
 - The snapshots only
- 7 From the drop-down menu, choose the iSCSI initiator group you want this volume to use.
- 8 From the drop-down menu, choose a CHAP account.
- 9 Click **Add**.
- 10 When you have finished assigning your volumes, click **Save**.

Assign Volumes to an iSCSI Initiator Group Using the CLI

You can assign an existing volume to an iSCSI initiator group using the CLI. You can also assign a volume to an iSCSI initiator group when you create the volume.

See "Create a Volume Using the GUI" or "Create a Volume Using the CLI" in the *Nimble Storage Installation Guide*.

Before you begin

You must create your iSCSI initiator groups before you can assign volumes to them.

Procedure

To assign a volume to an iSCSI initiator group in the CLI:

- 1 At the command prompt, type: **vol --addacl <volume name> --apply_acl_to <volume | snapshot | both> --initiatorgrp <initiatorgrp-name>**
Example: **vol --addacl volume1 --apply_acl_to both --initiatorgrp Dataman**
- 2 Type the following command to verify that the volume was assigned: **vol --info <volume name>**
Example: **vol --info volume1**

In the list of volume information, look for *Access Control List*. You should see a result like this:

```
Access Control List:
  Apply to: volume & snapshot
  Initiator Group: Dataman
  CHAP user: *
```

Unassign Volumes from an iSCSI Initiator Group Using the GUI

Procedure

To un-assign a volume from an iSCSI initiator group in the GUI:

- 1 From the home page, go to **Manage > Data Storage**.
- 2 On the Volumes page, check the volume you want to unassign from the iSCSI initiator group.
- 3 Click **Edit** (the pencil icon).
- 4 Click **Access** on the progress bar.
- 5 In the list, under *iSCSI Initiator Group*, find the iSCSI initiator group you want to un-assign, and click the X icon.
- 6 Click **OK** to confirm.
- 7 When you have finished un-assigning your volumes, click **Save**.

Unassign Volumes from an iSCSI Initiator Group Using the CLI

Procedure

To un-assign a volume from an iSCSI initiator group using the CLI:

- 1 At the command prompt, type **vol --removeacl <volume name> --apply_acl_to <volume | snapshot | both> --initiatorgrp <initiatorgrp-name>**.

Example: **vol --removeacl volume1 --apply_acl_to both --initiatorgrp Dataman**

- 2 Type **vol --info <volume name>** to verify that the volume was assigned.

Example: **vol --info volume1**

In the list of volume information, look for *Access Control List*. You should see a result like this:

```
Access Control List:
  Apply to: *
  Initiator Group: *
  CHAP user: *
```

Edit an iSCSI Initiator Group Using the GUI

To edit an iSCSI initiator group means any combination of:

- Adding client iSCSI initiators
- Removing client iSCSI initiators
- Adding subnets
- Removing subnets

Procedure

- 1 Choose **Manage > Data Access**.

- 2 Click the iSCSI group you want to modify and click **Edit** (the pencil icon).
The Edit Initiator Group dialog box opens.
- 3 (Optional) Under Target subnets, choose one of the options:
 - Use all configured subnets
 - Select target subnets
 If you chose Select target subnets, a list of available subnets appears.
- 4 (Optional) Under Available subnets, highlight the subnets you want to associate with this iSCSI initiator group and click **Add**.
- 5 (Optional) Under Available Subnets, highlight the subnets you want to disassociate with this iSCSI initiator group and click **Remove**.
- 6 (Optional) To add an iSCSI initiator, under Initiators:
 - a) Click **Add**.
 - b) Type a name for the initiator in the Name field.
 - c) Copy-and-paste the IQN of the client system into the IQN field.
Note If you cannot copy-and-paste the IQN, type it very carefully.
 - d) Enter the IP address of the client system in the IP Address field.
- 7 (Optional) To remove an iSCSI initiator:
 - a) Find the initiator you want to remove.
 - b) Click the X beside the initiator.
- 8 Click **Save**.

What to do next

Important

- If target subnets are added, rescan on ESX or refresh on Windows to connect to the new target subnets.
- If target subnets are removed, manually break the existing connections.
- If an initiator is removed or edited (change of IQN or IP address), manually break the existing connections.

Edit an iSCSI Initiator Group Using the CLI

Complete the step for the task you want to complete.

Procedure

- 1 Add an initiator to an initiator group.
`initiatorgrp --add_initiators initiatorgrp_name --label label --initiator_nameiqn --ipaddr client_ipaddr`
Note If you cannot copy and paste the IQN, type it very carefully.
- 2 Remove an initiator from an initiator group.
`initiatorgrp --remove_initiator initiatorgrp_name --label label`
- 3 Add a subnet to an initiator group.
`initiatorgrp --add_subnets initiatorgrp_name --label subnet_label`
- 4 Remove a subnet from an initiator group.
`initiatorgrp --remove_subnet initiatorgrp_name --label subnet_label`
- 5 (Optional) Verify your changes.
`initiatorgrp --info initiatorgrp_name`
 You should see a result like this:

```
Name: Dataman
Description:
Access Protocol: iscsi
Created: Feb 19 2014 16:16:32
Last configuration change: Feb 19 2014 16:16:32
Number of Subnets: 1
    Subnet Label: Subnet-198.51.100.0
Number of Initiators: 1
    Initiator Label: Basic
        Initiator Name: iqn.1991-05.com.microsoft:techops.storage.com
        Initiator IP Address: 198.0.2.88
```

Example

Adding an initiator.

```
Nimble OS $ initiatorgrp --add_initiators Dataman --label client1
--initiator_name iqn.1991-05.com.microsoft:techops.storage.com --ipaddr
192.0.2.88
```

Removing an initiator.

```
Nimble OS $ initiatorgrp --remove_initiator Dataman --label client1
```

Adding a subnet.

```
Nimble OS $ initiatorgrp --add_subnets Dataman --label Subnet-198.51.100.0
```

Removing a subnet.

```
Nimble OS $ initiatorgrp --remove_subnets Dataman --label
Subnet-198.51.100.0
```

Verifying the results.

```
Nimble OS $ initiatorgrp --info Dataman
```

What to do next

Important

- If target subnets are added, rescan on ESX or refresh on Windows, to connect to the new target subnets.
- If target subnets are removed, manually break the existing connections.
- If an initiator is removed or edited (change of IQN or IP address), manually break the existing connections.

Delete an iSCSI Initiator Group Using the GUI

Procedure

- 1 Choose **Manage > Data Access**.
- 2 On the Initiator Groups page, check the box to the left of the iSCSI group you want and click **Delete**.
- 3 Click **OK** to confirm.

Delete an iSCSI Initiator Group Using the CLI

Procedure

To delete an iSCSI initiator group:

- 1 At the command prompt, type **initiatorgrp --delete <initiator group name>**.

Example: **initiatorgrp --delete Dataman**

- 2 Type **initiatorgrp --list** to verify that the initiator group was deleted.

What to do next

Important Manually break the existing connections with the client.

Index

A

- about [103](#), [119](#)
 - discovery IP address [119](#)
 - SRA for SRM [103](#)
- ACLs [8](#)
- adapter, Serial-USB-VGA [134–135](#)
- add [50–51](#), [109](#), [137–138](#)
 - array to SRM [109](#)
 - iSCSI initiator group [137–138](#)
 - VMs [50–51](#)
- alignment of partitions [50](#)
- application-consistent quiescing, enable [132](#)

B

- bind vmk ports [29](#)
- block alignment [8](#)

C

- cable, null-modem or serial [134](#)
- clone [71](#), [86](#)
 - datastore [71](#), [86](#)
- cloning, rapid [57](#)
- configure [9](#), [15](#), [27](#), [113](#), [124](#), [127](#)
 - ESX datastore [127](#)
 - ESXi iSCSI adapter [27](#)
 - iSCSI discovery [113](#)
 - jumbo frames [124](#), [127](#)
 - multiple vSwitches [9](#)
 - single vSwitch [15](#)
- connected devices, list [113](#)
- connections [33](#), [119](#), [134–135](#)
 - direct [135](#)
 - iSCSI [33](#)
 - rebalance [119](#)
 - serial [134](#)
- copy NCM to ESXi host [37](#)
- create datastore [67](#), [81](#), [98](#)
- create VM [98](#)

D

- data ports [119](#)
- datastore [67](#), [71–75](#), [81](#), [86–87](#), [89–90](#), [94](#), [98](#), [127](#)
 - clone [71](#), [86](#)
 - create [67](#), [81](#), [98](#)
 - delete [75](#), [94](#)
 - edit [90](#)
 - ESX, configure [127](#)
 - grow [72](#), [87](#)
 - resize [72](#), [87](#)
 - take snapshot [74](#), [89](#)
- delete datastore [75](#), [94](#)
- details, view [73](#), [87](#)
- device list, Nimble LUNs [59](#)

- direct connection [135](#)
- disable [9](#), [15](#), [53](#)
 - NIC teaming [9](#), [15](#), [53](#)
- disaster recovery [95](#), [100](#)
 - VASA Provider [95](#), [100](#)
- discovery IP address [33](#), [59](#), [119](#)
- dongle [134–135](#)
- download [40](#), [105](#)
 - NCM [40](#)
 - SRA for SRM [105](#)

E

- edit datastore [90](#)
- enable [132](#)
 - application-consistent quiescing [132](#)
- ESX datastore, configure [127](#)
- ESX version required for vCenter plugin [78](#)
- ESXi iSCSI adapter [27](#)
 - configure [27](#)
- ESXi iSCSI networking [9](#), [15](#)
 - multiple vSwitches [9](#)
 - single vSwitch [15](#)
- ESXi version required for vCenter plugin [63](#)

F

- flow control [8](#)
- frame size, change [127](#)

G

- grow datastore [72](#), [87](#)

H

- host name, change [53](#)

I

- implement recovery plan [111](#)
- initiate recovery plan [110](#)
- install [38–39](#), [41–42](#), [106](#)
 - NCM [38–39](#), [41–42](#)
 - offline bundle [42](#)
 - online bundle [41](#)
 - Update Manager, offline [39](#)
 - Update Manager, online [38](#)
 - Nimble SRA for SRM [106](#)
 - SRA for SRM [106](#)
- installation prerequisites [36](#)
 - InfoSight credentials [36](#)
 - Internet connection [36](#)
 - SFTP client [36](#)
 - SSH client [36](#)
- IP address [33](#), [137–138](#)
 - discovery [33](#)

- IP address (*continued*)
 - iSCSI initiator group [137–138](#)
- iSCSI [33, 53, 113, 119, 124](#)
 - best practices [53](#)
 - configure [53](#)
 - connections [33](#)
 - discovery IP address [33](#)
 - discovery, configure [113](#)
 - host connection methods [119](#)
 - manual host connection, setting [124](#)
- iSCSI Digest [93–94](#)
 - disable [94](#)
 - enable [93](#)
- iSCSI initiator group [137–141, 143](#)
 - assign volumes [139](#)
 - create [137–138](#)
 - delete [143](#)
 - edit using the CLI [141](#)
 - un-assign volumes [140](#)
- iSCSI initiator groups [140, 142](#)
 - delete using the GUI [142](#)
 - edit using the GUI [140](#)
- iSCSI initiators [140–141](#)
 - add to initiator group using the CLI [141](#)
 - add to initiator group using the GUI [140](#)
 - remove from initiator group using the CLI [141](#)
 - remove from initiator group using the GUI [140](#)

J

- jumbo frames [8, 124, 127](#)
 - configure [124, 127](#)
 - support for [8](#)

K

- KVM port [134–135](#)

L

- list of plugins [64](#)
- logs [59](#)
- vCenter [59](#)

M

- manage target subnets [56](#)
- manage VVols [99](#)
- manual host connection method, setting [124](#)
- MTU, change size [127](#)

N

- NCM [33, 36–45](#)
 - configure [43](#)
 - copy to ESXi host [37](#)
 - disable [43](#)
 - download software [40](#)
 - enable [43](#)
 - install [38–39, 41–42](#)
 - offline bundle [42](#)

- NCM (*continued*)
 - install (*continued*)
 - online bundle [41](#)
 - Update Manager, offline [39](#)
 - Update Manager, online [38](#)
 - installation [36](#)
 - uninstall [45](#)
 - update [44](#)
 - verify installation [43](#)
- NCM configuration [43](#)
 - modify [43](#)
 - view [43](#)
- NCM logs [44](#)
 - view [44](#)
- NIC [9, 15, 53, 127](#)
 - change frame size [127](#)
 - teaming [9, 15, 53](#)
- Nimble [33, 105](#)
 - Connection Manager [33](#)
 - support downloads [105](#)
- Nimble Connection Manager [33](#)
 - NCM [33](#)
- Nimble SRA for SRM [103, 105–106, 109](#)
 - about [103](#)
 - add array [109](#)
 - high-level overview [103](#)
 - install [106](#)
 - prerequisites [105](#)
 - un-install [109](#)
 - versions [105](#)
- Nimble-specific roles [65, 78](#)
- NimbleOS [47](#)
 - excluding VMs, datastores from snapshots [47](#)
- NimbleSnapExclude [48](#)
 - tag to exclude VMs, datastores from snapshots [48](#)
- NimbleSnapInclude [48](#)
 - tag to include VMs, datastores from snapshots [48](#)
- NimbleVMwareSyncSnaps [47](#)
 - tag category for snapshots [47](#)
- null-modem cable [134](#)

O

- offline bundle, NCM installation [42](#)
- online bundle, NCM installation [41](#)
- overview, VMware iSCSI configuration [9](#)

P

- partition alignment [50](#)
- path selection policy [131](#)
- Permissions [65, 78](#)
- plugin, vCenter [63–64, 75–76, 94](#)
 - register [63–64](#)
 - in CLI [63](#)
 - in GUI [64](#)
 - unregister [75–76, 94](#)
 - in CLI [75](#)
 - in GUI [76](#)
 - in vCenter [76, 94](#)

- plugin, vCenter web client [78](#)
 - register [78](#)
 - in CLI, GUI [78](#)
- plugins, list [64](#)
- privileges [8](#)
- Protection Manager [49](#)

R

- rapid cloning [57](#)
- RBAC [65](#), [78](#)
- RDM [59](#)
- recovery plan [110–111](#)
 - implement [111](#)
 - initiate [110](#)
 - test [111](#)
- register vCenter plugin [63–64](#)
 - CLI [63](#)
 - GUI [64](#)
- register vCenter web plugin [78](#)
 - CLI, GUI [78](#)
- register VMs [50–51](#)
- replication partner [109](#)
- Reprotect [111](#)
- rescan storage adapters [59](#)
- resize datastore [72](#), [87](#)
- restore [51](#)
 - VMware volume from snapshot [51](#)
- Role-Based Access Control [100](#)
 - RBAC and VVols [100](#)
- roles [100](#)
 - administrator [100](#)
 - guest [100](#)
 - operator [100](#)
 - power user [100](#)
- Roles [65](#), [78](#)
- round robin [131](#)

S

- serial connection [134](#)
- Serial-USB-VGA adapter [134–135](#)
- SFTP client [37](#)
- single vSwitch, configure [15](#)
- snapshots [46–49](#), [51–52](#), [74](#), [89](#)
 - application-consistent [49](#)
 - assign tags to VMs, datastores [48](#)
 - create a tags category [47](#)
 - create exclude, include tags for VMs, datastores [48](#)
 - datastore [74](#), [89](#)
 - excluding VMs, datastores [47](#)
 - in VMware [46](#)
 - restore VMware volume from [52](#)
 - restoring VMware volume from [51](#)
 - with VMware [46](#)
- SRA for SRM [103](#), [105–107](#), [109](#)
 - about [103](#)
 - add array [109](#)
 - download [105](#)
 - high-level overview [103](#)
 - install [106](#)
 - prerequisites [105](#)

- SRA for SRM (*continued*)
 - un-install [109](#)
 - update [107](#)
 - versions [105](#)
- SRA with VSS [112](#)
- SRM [103](#)
 - high-level overview [103](#)
- SSH client [41–43](#), [107](#)
- storage adapters, rescan [59](#)
- Storage Policy-Based Management (SPBM) [95](#)
 - VASA Provider [95](#)
- subnet [140](#)
- subnets [140–141](#)
 - add to initiator group using the CLI [141](#)
 - add to initiator group using the GUI [140](#)
 - remove from initiator group using the CLI [141](#)
 - remove from initiator group using the GUI [140](#)

T

- tags [47–48](#)
 - create exclude, include snapshot tags for VMs, datastores [48](#)
 - creating a category [47](#)
- target subnets [56](#)
 - manage [56](#)
- test [111](#)
 - recovery plan [111](#)
- troubleshooting [101](#)

U

- un-install [109](#)
 - SRA for SRM [109](#)
- uninstall [45](#)
 - NCM [45](#)
- unregister vCenter plugin [75–76](#), [94](#)
 - CLI [75](#)
 - GUI [76](#)
 - vCenter [76](#), [94](#)
- update [44](#), [107](#)
 - NCM [44](#)
 - SRA for SRM [107](#)
- Update Manager, NCM installation [38](#)
 - online [38](#)
- username and password for CLI [134–135](#)

V

- VAAI [61](#)
 - defined [61](#)
 - integration [61](#)
- VAAI primitives [61](#)
 - ATS [61](#)
 - block delete [61](#)
 - extended copy [61](#)
 - thin provisioning stun [61](#)
 - UNMAP [61](#)
 - write same [61](#)
 - XCOPY [61](#)
 - zero blocks [61](#)

- VAAI providers [61](#)
 - enable [61](#)
 - VMware [61](#)
- VASA Provider [95](#), [100](#)
 - disaster recovery [95](#), [100](#)
 - Storage Policy-Based Management (SPBM) [95](#)
 - VVols [95](#), [100](#)
- vCenter [46](#), [53](#), [59–60](#)
 - change host name [53](#)
 - logs [59](#)
 - unresponsive [60](#)
 - works with array [46](#)
- vCenter plugin [63–64](#), [75–76](#), [78](#), [94](#)
 - ESX version required [78](#)
 - ESXi version required [63](#)
 - list [64](#)
 - register in CLI [63](#)
 - register in GUI [64](#)
 - unregister in CLI [75](#)
 - unregister in GUI [76](#)
 - unregister in vCenter [76](#), [94](#)
- vCenter web plugin [78](#)
 - register in CLI, GUI [78](#)
- VDI [61](#)
- verify NCM installation [43](#)
- VIB [8](#)
- view [64](#), [73](#), [87](#), [113](#)
 - datastore details [73](#), [87](#)
 - list of connected devices [113](#)
 - list of plugins [64](#)
 - paths to volume [113](#)
- VM [50–51](#), [53](#), [98](#), [132](#)
 - add/register [50–51](#)

- VM (*continued*)
 - create [98](#)
 - guest machine [53](#)
 - Windows Server 2008 [132](#)
- VM guest machines [54](#)
 - iSCSI VMkernel ports [54](#)
 - VMkernel ports [54](#)
- VM NIC [59](#)
- vmk ports, bind [29](#)
- VMware [8–9](#), [46–47](#), [49](#)
 - Accepted [8](#)
 - excluding VMs, datastores from snapshots [47](#)
 - iSCSI configuration [9](#)
 - objects [49](#)
 - synchronized snapshots [46](#)
 - VSS services support [46](#)
- volume [139–140](#)
 - assign to iSCSI initiator group [139](#)
 - unassign from iSCSI initiator group [140](#)
- volume collections [49](#)
- volumes [52](#)
 - restore from snapshot [52](#)
- VSS with SRA [112](#)
- VVols [97](#), [99–100](#)
 - manage [99](#)
 - using VASA Provider for disaster recovery [100](#)
 - workflow [97](#)

W

- workflow [97](#)
- VVols [97](#)