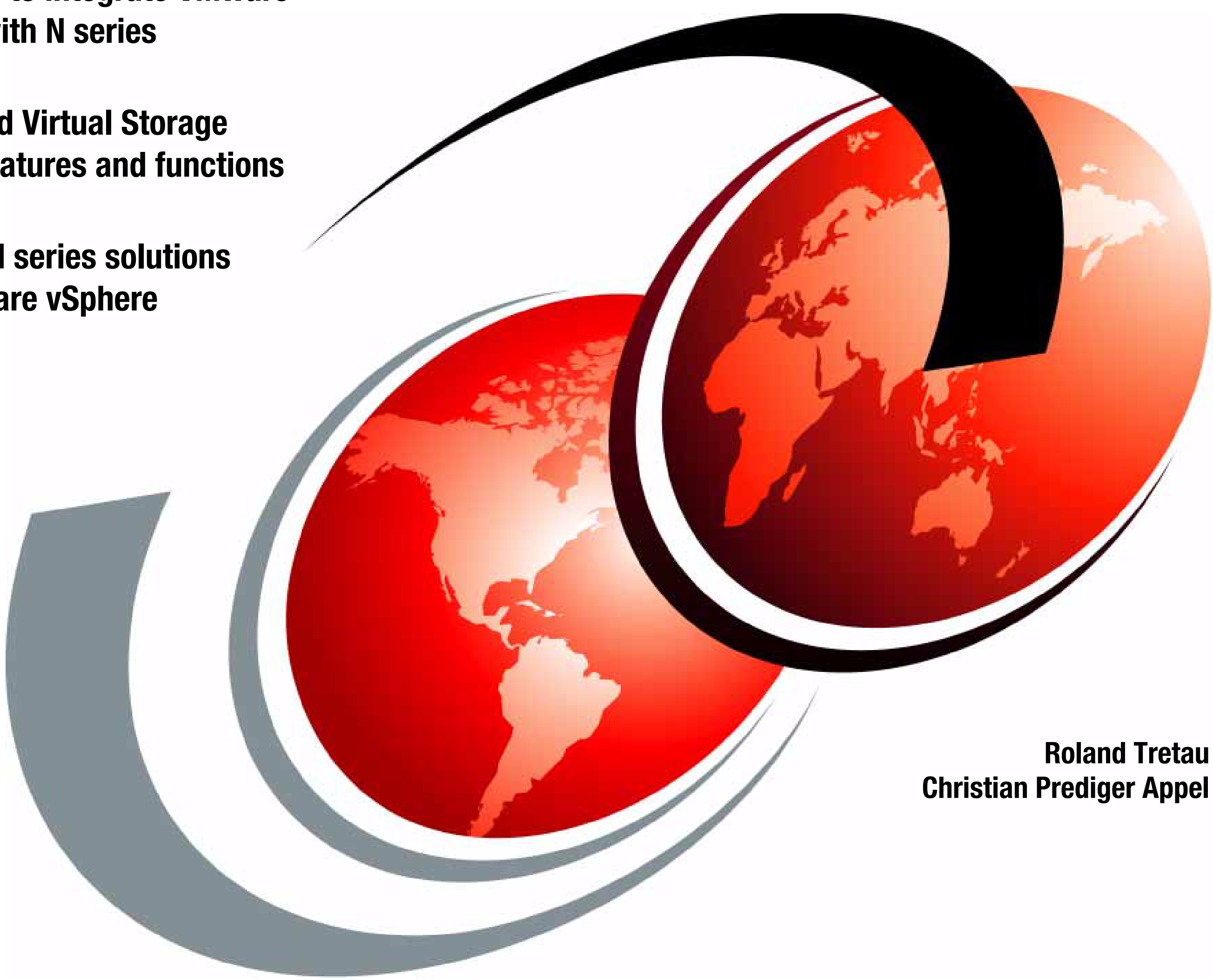
# IBM System Storage N series with VMware vSphere 4.1

Learn how to integrate VMware vSphere with N series

Understand Virtual Storage Console features and functions

Optimize N series solutions with VMware vSphere



Roland Tretau
Christian Prediger Appel

Redbooks

ibm.com/redbooks

International Technical Support Organization

**IBM System Storage N series with VMware vSphere 4.1**

February 2012

SG24-7636-02

**Note:** Before using this information and the product it supports, read the information in “Notices” on page xxi.

**Third Edition (February 2012)**

This edition applies to Data ONTAP 7.3.6 and later.

# Contents



# Figures



# Tables

# Examples



# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
*IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

# Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

| | | |
|---|---|---|
| DB2® | Redbooks® | Tivoli® |
| HiperSockets™ | Redbooks (logo) ® | |
| IBM® | System Storage® | |

The following terms are trademarks of other companies:

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Snapshot, RAID-DP, LockVault, FlexShare, SyncMirror, SnapVault, SnapRestore, SnapMover, SnapMirror, SnapManager, SnapLock, SnapDrive, NearStore, MultiStore, FlexVol, FlexClone, FilerView, Data ONTAP, NetApp, and the NetApp logo are trademarks or registered trademarks of NetApp, Inc. in the U.S. and other countries.

SUSE, the Novell logo, and the N logo are registered trademarks of Novell, Inc. in the United States and other countries.

QLogic, and the QLogic logo are registered trademarks of QLogic Corporation. SANblade is a registered trademark in the United States.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

# Preface

This IBM® Redbooks® publication provides a basic introduction to the IBM System Storage® N series, virtualization, and VMware. It explains how to use the N series with VMware vSphere 4 environments and the benefits of doing so. Examples are given on how to install and set up VMware ESXi server with the N series.

This edition includes information about the Virtual Storage Console (VSC), which is another N series software product that works with VMware. VSC provides local backup and recovery capability with the option to replicate backups to a remote storage system by using SnapMirror relationships. Backups can be performed on individual virtual machines or on datastores. You have the option of updating the SnapMirror relationship as part of the backup on a per job basis. Similarly, restores can be performed at a data-store level or individual virtual machine level.

IBM System Storage N series in conjunction with VMware vSphere 4 helps complete the virtualization hierarchy by providing both a server and storage virtualization solution. Although this configuration can further assist with other areas of virtualization, networks, and applications, these areas of virtualization are not covered in detail in this book.

**VMware ESX terminology:** A VMware ESX Server is often referred to as a *VMware host* (the host), and the virtual servers running on the host are often called *guests*. This IBM Redbooks publication follows this naming method.

## The team who wrote this book

This book was produced by a team of specialists from around the world working at the IBM European Storage Competence Center (ESCC) located in Mainz, Germany. The work was done in close cooperation with the International Technical Support Organization (ITSO), San Jose, California, USA.

**Roland Tretau** is an Information Systems professional with IBM in Germany and has over 15 years of experience in the IT industry. Roland has a solid background in project management, consulting, operating systems, storage solutions, enterprise search technologies, and data management. He holds Engineering and Business Masters degrees and is the author of many storage-related Redbooks publications.

**Christian Prediger Appel** is a Server Specialist in Global Technology Services. He provided expert knowledge with servers, network, and storage components since 2000. Christian worked for an Internet Service Provider (ISP) and a server management company before joining IBM in 2005, where he works managing and implementing server projects. His expertise is in virtualization of infrastructure and applications. In addition, Christian holds several certifications from Microsoft, Citrix, VMware, and is an IBM certified IT Specialist.

- Authors of previous editions of this book were:
  - Norm Bogard
  - Gil Pastrana
  - Amrita Das
  - Ricardo Hortencio
  - Vicky Rose
  - Michael Slisinger

Thanks to the following people for their contributions to this project:

Uwe Heinrich Mueller, Uwe Schweikhard
IBM Germany

Jürgen Mutzberg, Erwin Breneis
VMWare

## Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

**ibm.com**/redbooks/residencies.html

## Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  **ibm.com**/redbooks

- Send your comments in an e-mail to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

## Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

# Summary of changes

This section describes the technical changes made in this edition of the book and in previous editions. This edition might also include minor corrections and editorial changes that are not identified.

Summary of Changes
for SG24-7636-02
for *IBM System Storage N series with VMware vSphere 4.1*
as created or updated on April 8, 2012.

## February 2012, Third Edition

This revision reflects the addition, deletion, or modification of new and changed information described below.

### Updated information

We added the following updates to this Redbooks publication:

- Updated with the latest N series model and feature information.
- Updated to reflect VMware vSphere 4.1 environments

### New information

We added the following updates to this Redbooks publication:

- Information for Virtual Storage Console 2.x has been added

1

# Introduction to IBM System Storage N series

The IBM System Storage N series offers an additional choice for organizations that are facing the challenges of enterprise data management. The IBM System Storage N series delivers high-end value with midrange affordability. Built-in enterprise serviceability and manageability features help to support customer efforts to increase reliability, simplify and unify storage infrastructure and maintenance, and deliver exceptional economy.

## 1.1 Unified storage

The IBM System Storage N series storage systems offer multiprotocol connectivity by using internal storage or storage provided by expansion units, as shown in Figure 1-1. The N series systems are designed to provide integrated block-level and file-level data access, allowing concurrent operation in IP SAN (iSCSI), FC SAN, NFS, and CIFS environments.

Other storage vendors might require the operation of multiple systems to provide this functionality. N series storage systems are designed to avoid costly downtime, both planned and unplanned, and improve your access to important data, helping you gain a competitive advantage. Features and functions provide data protection and data recovery solutions for customers' business critical environment as well as foundations for cloud storage solutions.

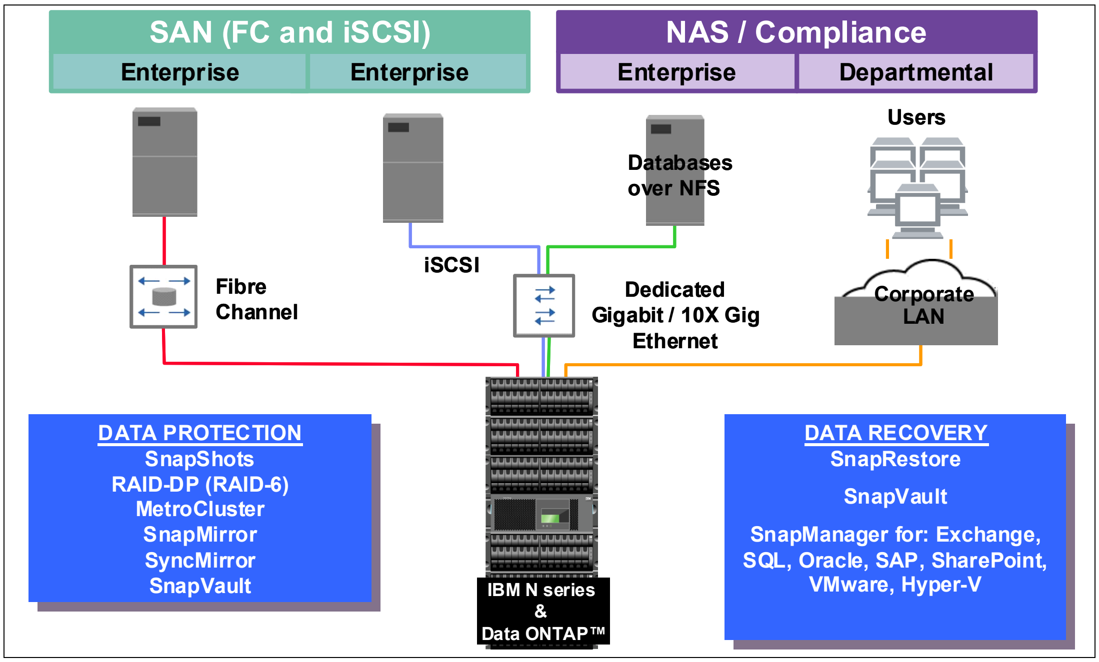



*Figure 1-1 N series unified storage*

The N series is a specialized, *thin server* storage system with a customized operating system, similar to a stripped-down UNIX kernel, referred to as *Data ONTAP*. With this customized operating system, many of the server operating system functions that you are familiar with are not supported. Data ONTAP improves performance and reduces costs by eliminating unnecessary functions that do not pertain to a storage system.

N series units come with preconfigured software and hardware, and with no monitor or keyboard for user access, which is commonly called a *headless system*. A storage administrator accesses the systems and manages the disk resources from a remote console by using a web browser or command line.

A typical characteristic of an N series storage systems product is its ability to be installed rapidly, using minimal time and effort to configure the system. The N series product is integrated seamlessly into the network, making it especially attractive when time and skills are limited in the organization of the customer.

## 1.2 Product overview

The IBM System Storage N series portfolio (Figure 1-2) provides a range of reliable, scalable storage solutions for various storage requirements. These capabilities are achieved by using network access protocols. Examples include Network File System (NFS), Common Internet File System (CIFS), HTTP, and iSCSI, as well as storage area network (SAN) technologies such as Fibre Channel (FC).

By using built-in Redundant Array of Independent Disks (RAID) technologies, all data is well protected, with options to enhance protection through mirroring, replication, snapshots, and backup. These storage systems are also characterized by simple management interfaces that make installation, administration, and troubleshooting straightforward.

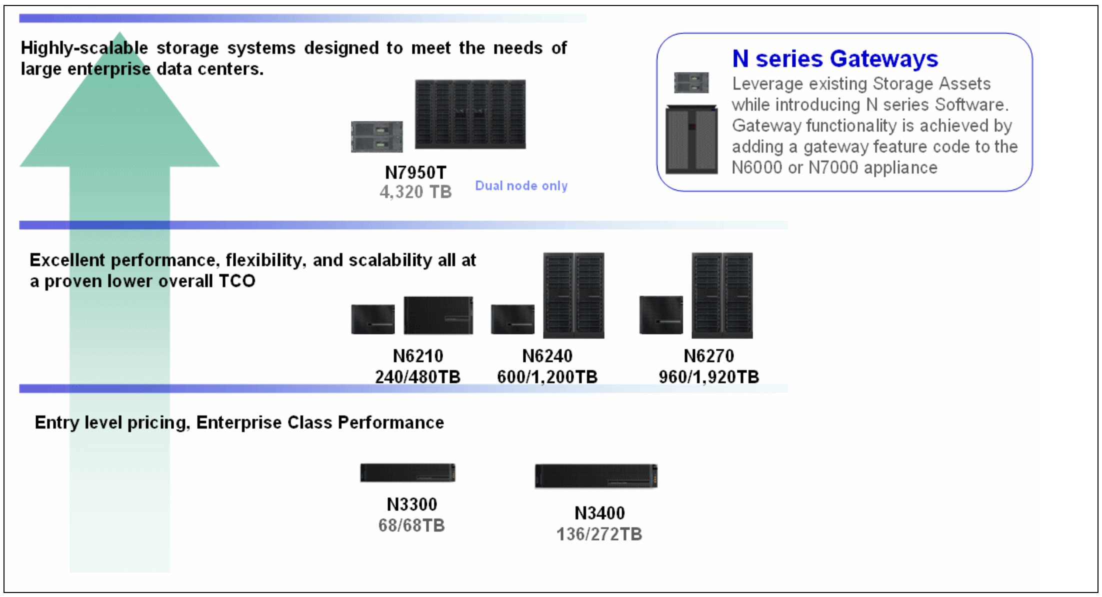



*Figure 1-2 N series portfolio*

The most current IBM System Storage N series portfolio can be found at:

http://www.ibm.com/systems/storage/network/hardware/index.html

With this type of flexible storage solution, you can perform the following tasks:

- Tune the storage environment to a specific application while maintaining flexibility to increase, decrease, or change access methods with minimal disruption.
- React easily and quickly to changing storage requirements. If additional storage is required, you can expand it quickly and non-disruptively. If existing storage is deployed incorrectly, you can reallocate available storage from one application to another quickly and simply.
- Maintain availability and productivity during upgrades. If outages are necessary, they can be kept to the shortest time possible.
- Create effortless backup and recovery solutions that operate in a common manner across all data access methods.
- Simplify your infrastructure with file- and block-level services in a single system.
- Tune the storage environment to a specific application while maintaining its availability and flexibility.
- Change the deployment of storage resources non-disruptively, easily, and quickly. Online storage resource redeployment is possible.
- Easily and quickly implement the upgrade process. Non-disruptive upgrade is possible.
- Achieve strong data protection solutions with support for online backup and recovery.
- Include added value features, such as N series deduplication and IBM Real-time Compression, to optimize space management.

All N series storage systems use a single operating system across the entire platform. They offer a combination of multiple advanced function software features that provide one of the most multifaceted storage platforms in the industry. Such features include comprehensive system management, storage management, onboard copy services, virtualization technologies, and disaster recovery and backup solutions.

## 1.3 High availability as a cloud foundation

N series systems are available as clusters and are also referred to as active-active HA pairs. These consist of two independent storage controllers that provide fault tolerance and high-availability storage for virtual environments. The cluster mechanism provides nondisruptive failover between controllers in the event of a controller failure. Redundant power supplies in each controller maintain constant power. Storage HBAs and Ethernet NICs are all configured redundantly within each controller. The failure of up to two disks in a single RAID group is accounted for by RAID-DP.

The N series active-active HA cluster model can be enhanced by synchronously mirroring data at the RAID level using NetApp SyncMirror. This mirrored active-active configuration maintains two complete copies of all mirrored data. These copies are called plexes and are continually and synchronously updated every time Data ONTAP writes to a mirrored aggregate. When SyncMirror is used with HA clustering, the cluster has the ability to survive the loss of complete RAID groups or shelves of disks on either side of the mirror.

MetroCluster builds on the N series cluster model by providing the capability to place the nodes of the clusters at geographically dispersed locations. Similar to the mirrored active-active configuration, MetroCluster also maintains two complete copies of all mirrored data. These copies are called plexes and are continually and synchronously updated each time Data ONTAP writes data to the disks.

MetroCluster supports distances of up to 100 kilometers. For distances less than 500 meters, the cluster interconnects, controllers, and disk shelves are all directly connected. This is referred to as a stretch MetroCluster configuration.

For distances over 500 meters, MetroCluster uses redundant Fibre Channel switches and interswitch links (ISL) between the sites. This configuration is referred to as a fabric MetroCluster configuration. In this case, the controllers and the storage are connected through the ISLs.

Note that the foregoing figures used in this section are simplified representations and do not indicate the redundant connection between each component. Figure 1-3 illustrates MetroCluster at more than 500 meters.

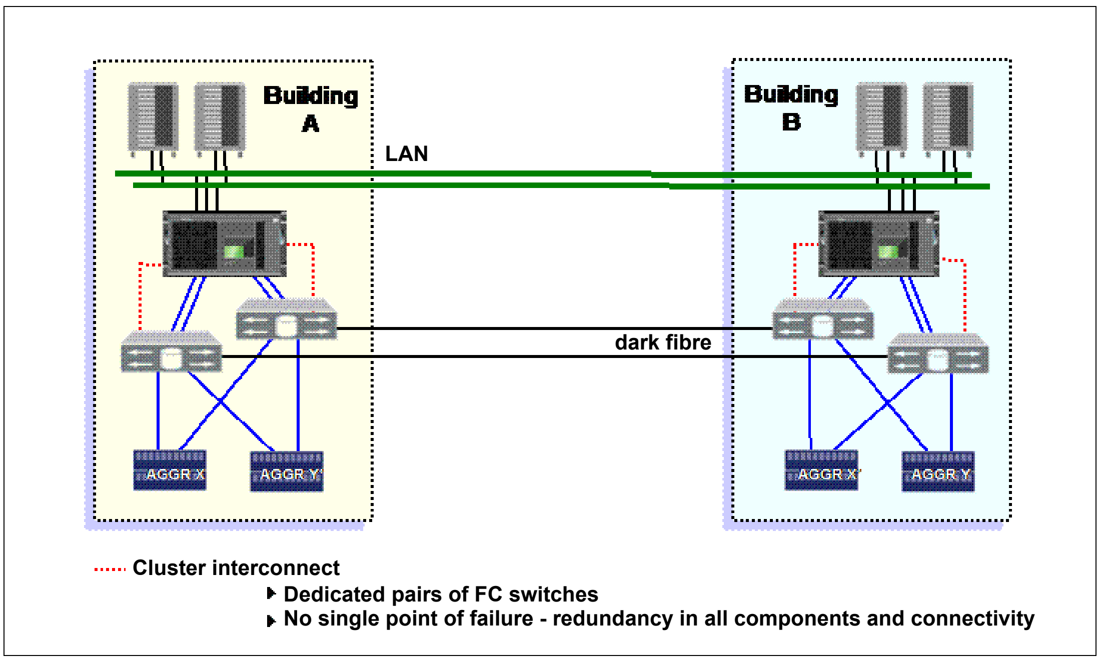



*Figure 1-3 MetroCluster greater than 500 meters*

## 1.4 N series software features

The IBM System Storage N series also provides a selection of features and functions designed to provide a comprehensive set of robust management and operational tools. This includes high availability features, disaster recovery, and data copy services. Such features help the system administration provide a high level of support for environments requiring IP attached storage solutions.

Figure 1-4 provides brief highlights of the available N series software features.

| | Software/Feature | Function | Benefit |
|---|---|---|---|
| Storage Efficiency | Deduplication | General-purpose deduplication for removal of redundant data objects | Reduces the amount of storage you need to purchase and maintain |
| | FlexClone | Instantaneously creates file, LUN and volume clones without requiring additional storage | Saves you time in testing and development and increases your storage capacity |
| | FlexVol | Creates flexibly sized LUNs and volumes across a large pool of disks and one or more RAID groups | Ensures that your storage systems are used at maximum efficiency and reduces your hardware investment |
| Backup & Recovery | Snapshot | Makes incremental, data-in-place, point-in-time copies of a LUN or volume with minimal performance impact | Enables you to create frequent, space efficient backups with no disruption to data traffic |
| | SnapRestore® | Rapidly restores single files, directories, or entire LUNs and volumes from any Snapshot backup | Instantaneously recovers your files, databases, and complete volumes from your backup |
| | SnapVault | Exports Snapshot copies to another IBM system, providing an incremental block-level backup solution | Provides you with cost-effective, long-term backups of disk-based data |
| | SnapLock | Write-protects structured application data files within a volume to provide WORM disk storage | Provides you with worry-free compliance with records retention regulations |
| | SnapMirror | Enables automatic, incremental data replication between systems: synchronous or asynchronous | Provides you with flexibility and efficiency when mirroring for data distribution and disaster recovery |
| | SyncMirror | Maintains two online copies of data with RAID-DP protection on each side of the mirror | Protects your system from all types of hardware outages, including triple disk failure |
| System Manageability | Operations Manager | Manages multiple IBM systems from a single administrative console | Simplifies your IBM deployment and allows you to consolidate management of multiple IBM systems |
| | Protection Manager | Backup and replication management software for IBM disk-to-disk environments | Lets you automate data protection, ensuring that you have mistake-free backup |
| | System Manager | Provides setup, provisioning and configuration management of a Data ONTAP storage system | Simplifies out-of-box setup and device management using an intuitive Windows based interface |

*Figure 1-4 Key N series software features*

## 1.5 IBM System Storage N series Gateways

The IBM System Storage N series Gateway product line is a network-based integrated storage solution. It provides Internet Protocol (IP) and Fibre Channel protocol access to SAN-attached heterogeneous storage arrays. The N6000 and N7000 series ordered with a Gateway feature code help you make the most of the dynamic provisioning capabilities of Data ONTAP software across your existing Fibre Channel SAN infrastructure to support an expanded set of business applications.

An N series Gateway implementation can be thought of as a front-end implementation and a back-end implementation. A front-end setup includes configuring the N series Gateway for all protocols (NAS or FCP) and implementing any snap features (such as Snapshot, SnapMirror, SnapVault, and so on). It also includes setting up backup, including NDMP dumps to tapes. The back-end implementation includes all tasks that are required to set up the N series Gateway system up to the point where it is ready for Data ONTAP installation. These tasks include array LUN formatting, port assignment, cabling, switch zoning, assigning LUNs to the N series Gateway system, creating aggregates, and loading Data ONTAP.

The IBM System Storage N series Gateway can provide network shares, exports, or LUNs that are built on flexible volumes that reside on aggregates. The N series Gateway is also a host on the storage array SAN. N series Gateways can take storage array LUNs (which are treated as disks) and virtualize them through Data ONTAP, presenting a unified management interface.

This simple, elegant data management solution can decrease management complexity and improve asset utilization. This solution also can streamline operations to increase business agility and reduce total cost of ownership and enhance data protection. In addition, it can enable rapid recovery and broaden centralized storage usage by provisioning SAN capacity for business solutions requiring NAS, SAN, or IP SAN data access (Figure 1-5).

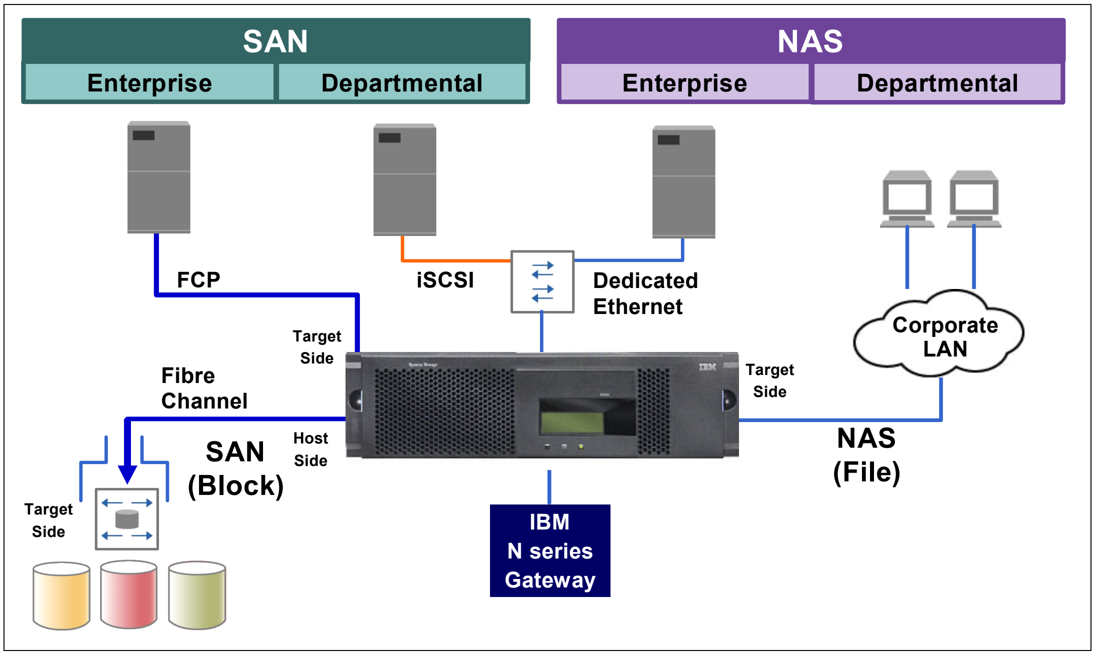



*Figure 1-5 Gateway topology*

With Data ONTAP, the N series Gateway now supports attachment of heterogeneous storage systems and IBM expansion units of the type used with N series storage systems.

IBM System Storage N series Gateway provides several key features that enhance the value and reduce the management costs of using a storage area network. An N series Gateway offers the following advantages:

- Simplifies storage provisioning and management
- Lowers storage management and operating costs
- Increases storage utilization
- Provides comprehensive, simple-to-use data protection solutions
- Improves business practices and operational efficiency
- Transforms conventional storage systems into a better managed storage pool (Figure 1-6)

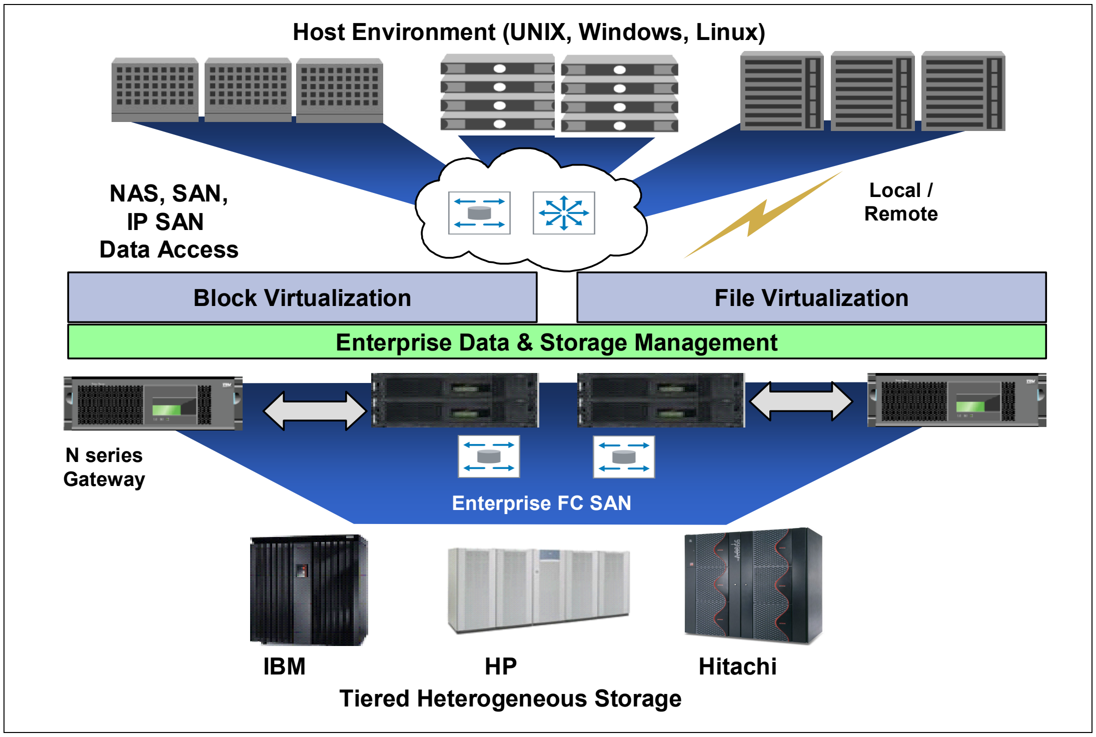



*Figure 1-6 Tiered heterogeneous storage*

Current N series interoperability matrices, included storage subsystems that are supported as N series back-end, are located at this website:

http://www.ibm.com/systems/storage/network/interophome.html

## 1.6 N series disk shelf technology

Currently four disk storage expansion units are available for the IBM System Storage N series storage systems:

- EXN4000: 4-Gbps Fibre Channel Disk Storage Expansion Unit (MTM 2863-004) with 14 low-profile slots for Fibre Channel disk drives
- EXN3500: SAS Small Form Factor (SFF) Disk Storage Expansion Unit (MTM 2857-006) with 24 SFF slots for SAS SFF disk drives
- EXN3000: SAS Disk Storage Expansion Unit (MTM 2857-003) with 24 slots for SAS disk drives
- EXN1000: SATA Disk storage expansion unit (MTM 2861-001) with 14 low-profile slots for SATA disk drives

**EXN expansion units:** EXN expansion units can be used for attachment to a Gateway with Data ONTAP 7.3 and later.

Multiple EXN1000s, each with different SATA disk drive feature codes, can be attached to the same N series storage system on the same Fibre Channel loop. Multiple EXN4000s, each with different Fibre Channel disk drive feature codes, can be attached to the same N series storage system on the same Fibre Channel loop. Multiple EXN3500s or EXN3000s, each with SAS or SATA disk drives, can be attached to the same N series storage system on the same SAS loop.

For the latest storage expansion unit support information, visit the IBM support website:

http://www.ibm.com/storage/support/nas/

An overview of current disk shelf technology is displayed in Figure 1-7.

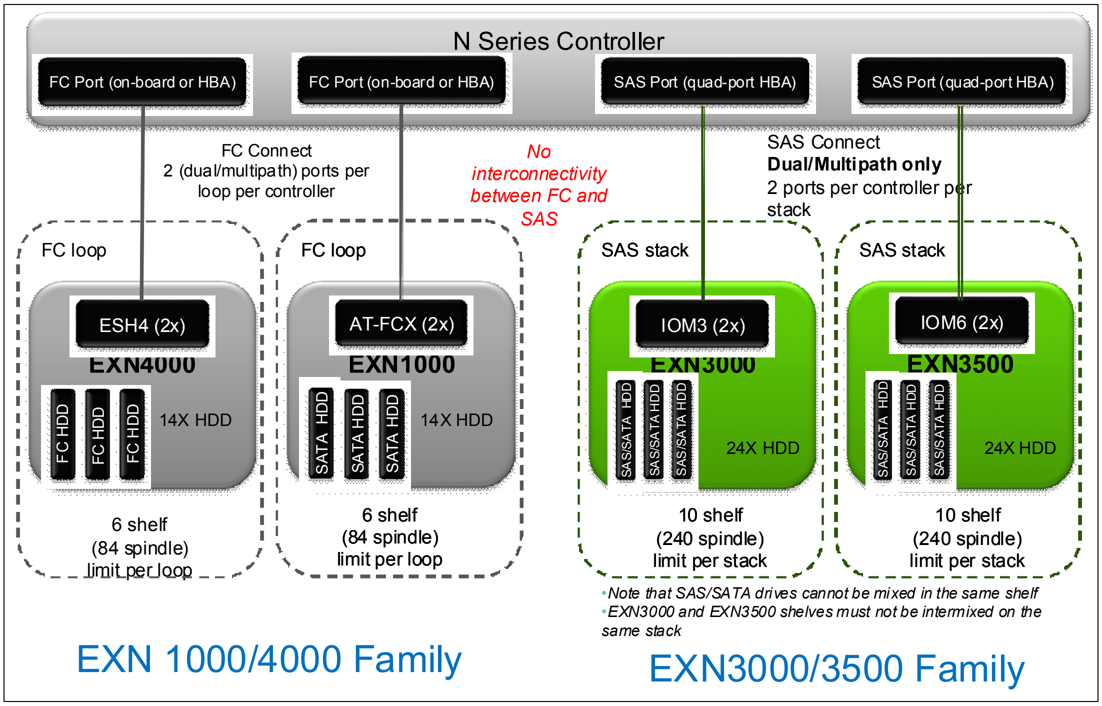



*Figure 1-7 Shelf topology comparison*

## 1.7 Hardware summary

The hardware portfolio can be categorized in three major segments: entry systems represented by the N3000 series, mid-range systems represented by the N6000 series, and enterprise systems represented by the N7000 series.

### 1.7.1 N3000 series

The IBM System Storage N3000 systems are designed to provide primary and secondary storage for midsize enterprises. This consolidates all of their fragmented application-based storage and unstructured data into one single-code system. Easily managed and expandable, this platform can help IT generalists increase their effectiveness.

In a cost-effective package, N3000 systems offer features such as those found in higher-end IBM System Storage N series systems:

- Integrated data access
- Intelligent management software
- Data protection capabilities

N3000 series innovations include internal controller support for the following capabilities:

- Serial-attached SCSI (SAS) or serial advanced technology attachment (SATA) drives
- Expandable I/O connectivity
- Onboard remote management

The N3000 series is compatible with the entire family of N series storage systems. These systems feature a comprehensive line-up of hardware and software designed to address a variety of possible deployment environments.

The N3300 series squeezes 24 TB of internal raw capacity into a 2U enclosure. Optional external expansion can increase total system raw capacity to 136 TB. The new N3400 series can expand up to 24 TB of internal raw capacity and increase total raw capacity to 272 TB. Whether used for primary or secondary storage, the N3000 Express systems are intended to provide outstanding deployment versatility and connectivity. This can help satisfy your data protection and recovery needs at an affordable cost, improving storage efficiency.

### 1.7.2 N6000 series

The IBM N6000 series offers extraordinary performance to help you meet demanding service levels of critical applications that can take priority under peak load conditions with FlexShare quality of service software. The Performance Acceleration Module (Flash Cache), an intelligent read cache, improves throughput and reduces latency to optimize the performance of your storage system. The N6000 series systems support simultaneous host attachment via CIFS, NFS, iSCSI and Fibre Channel protocols. The N6000 series supports up to 960 disk drives with a maximum raw capacity of 2880 TB.

### 1.7.3 N7000 series

The IBM System Storage N7000 series is designed to offer outstanding performance and expandability. It delivers high-end enterprise storage and data management value with midrange affordability.

## 1.7.4 At a glance

In summary, Figure 1-8 provides a hardware overview of current systems and disk shelves.

| IBM MODELS | N3300 | N3400 | N6210 | N6240 | N6270 | N7950T |
|---|---|---|---|---|---|---|
| NetApp Models | FAS2020 | FAS2040 | FAS3210 | FAS3240 | FAS3270 | FAS6280 |
| **System Storage N series Gateway** | | | | | | |
| IBM Model Numbers (s-single, c-clustered) | N/A | N/A | 2858-C10 (s)*<br>2858-C20 (c)*<br>*w/ feature code 9551 | 2858-E11 (s)*<br>2858-E21 (c)*<br>2858-C21 (c)*<br>*w/ feature code 9551 | 2858-E12 (s)*<br>2858-E22 (c)*<br>2858-C22 (c)*<br>*w/ feature code 9551 | 2867-E22(c)<br>*w/ feature code 9551 |
| FC Max | N/A | N/A | 144TB | 360TB | 576TB | 864TB |
| SATA Max | N/A | N/A | 720TB | 1800TB | 2880TB | 4320TB |
| **System Storage N series** | | | | | | |
| IBM Model Numbers (s-single, c-clustered) | 2859-A10(s)<br>2859-A20(c) | 2859-A11(s)<br>2859-A21(c) | 2858-C10 (s)<br>2858-C20 (c)<br>*w/feature code 9551 | 2858-E11 (s)<br>2858-E21 (c)<br>2858-C21 (c) | 2858-E12 (s)<br>2858-E22 (c)<br>2858-C22 (c) | 2867-E22 (c) |
| Memory/RAM¹ | 1GB | 4GB | 4/8GB | 8/16GB | 16/32GB | 192GB |
| Memory/Nonvolatile¹ | 128MB | 256MB | 512MB | 1GB | 1GB | 8GB |
| Max. Raw Capacity | 68TB | 136TB | 720TB | 1800TB | 2880TB | 4320TB |
| Max. Disk Drives | 68 | 136 | 240 | 600 | 960 | 1440 |
| Max LUNs | 1024 | 1024 | 2048 | 2048 | 2048 | 4096 |
| Form Factor: Single Controller | 2RU | 2RU | 3U | 3U | 3U | N/A |
| Form Factor: Clustered Pair | 2RU | 2RU | 3U | 3U or 6U | 3U or 6U | 12U |
| Drive Options: FC | 450/600GB | 450/600GB | 450/600GB | 450/600GB | 450/600GB | 450/600GB |
| Drive Options: SATA | 1TB/2TB/3TB | 1TB/2TB/3TB | 1TB/2TB/3TB | 1TB/2TB/3TB | 1TB/2TB/3TB | 1TB/2TB/3TB |
| Drive Options: SAS | 300/450/600GB | 300/450/600GB | 300/450/600GB & 100GB SSD | 300/450/600GB & 100GB SSD | 300/450/600GB & 100GB SSD | 300/450/600GB & 100GB SSD |
| Onboard/Max. Ports³: Ethernet, 1Gb | 4/4 | 8/8 | 4/20 | 4/52 | 4/52 | –/52 |
| Onboard/Max. Ports³: Ethernet, 10Gb | – | – | –/8 | –/24 | –/24 | 8/40 |
| Onboard/Max. Ports³: Fibre Channel, 4Gb | 4/4 | 4/4 | 4/20 | 4/52 | 4/52 | 8/48 |
| PCI-X/PCI-Express Expansion Slots² | – | – | 4 | 12 | 12 | 24 |

| EXPANSION SHELVES | Max. Disk Drives | Disk Drive Capacities | Disk Drive Type/Size | Interface Modules | Interface Type | Power Supply | Form Factor |
|---|---|---|---|---|---|---|---|
| **EXN1000** (NetApp DS14MK2AT) 2861-001 | 14 | 1TB 7.2K<br>2TB 7.2K | SATA | 2 x AT-FCX | 2Gb Fibre Channel | AC | 3RU |
| **EXN3000** (NetApp DS4243) 2857-003 | 24 | 1TB 7.2K, 2TB 7.2K, 3TB 7.2K 300GB 15K, 450GB 15K, 600GB 15K, 100GB SSD | SATA/SAS | 2 x IOM3 | 12Gb SAS | AC | 4RU |
| **EXN3500** (NetApp DS2246) 2857-006 | 24 | 450GB 10K<br>600GB 10K | SAS | SAS | 24Gb SAS | AC | 2U |
| **EXN4000** (NetApp DS14MK4FC) 2863-004 | 14 | 450GB 15K<br>600GB 15K | FC | 2 x ESH4 | 4Gb Fibre Channel | AC | 3RU |

¹ Single controller configuration
² Dual controller specifications
³ Onboard FC ports for N3300/N3600 can be used for either target (SAN) and/or initiator (disk) mode
⁴ The second number refers to dual controller specifications
⁵ N3400 has one embedded SAS port (2 in HA configuration)

*Figure 1-8 N series product portfolio overview*

## 1.8 Additional N series resources

For more details about N series hardware and software features, including an in-depth explanation of functions, see the following Redbooks publications:

- IBM System Storage N series Hardware Guide, SG24-7840

  http://www.redbooks.ibm.com/abstracts/sg247840.html?Open

- IBM System Storage N series Software Guide, SG24-7129

  http://www.redbooks.ibm.com/abstracts/sg247129.html?Open

2

# Introduction to virtualization

Virtualization helps you take control of your infrastructure. With virtualization, you can see and manage your computing resources in ways that offer more flexibility because you are not restricted by implementation, location, or physical packaging. By using virtualization, you have a logical, rather than a physical, view of data, computing power, storage capacity, and other resources. By gaining greater control of your infrastructure, you can improve cost management.

This chapter describes the various types of virtualization. It includes the following topics:

- Advantages of virtualization
- Storage virtualization
- Network virtualization
- Application virtualization
- Server virtualization

## 2.1 Advantages of virtualization

Businesses are pursuing financial savings through both server and storage consolidation. The consolidation is achieved by using virtualization. *Virtualization* is the abstraction of a physical resource into a virtual resource that is decoupled from the underlying hardware. Consolidation of server and storage hardware by using virtualization offers a return on investment (ROI) for the business.

Although cost savings is a primary driver for initial virtualization deployment, the full value of virtualization lies in its ability to offer the following advantages:

- Improved total cost of ownership (TCO):

  By decreasing management costs and increasing asset utilization, you can experience a rapid ROI with virtualization. In addition, by virtualization of resources, you can make them easier to migrate or fail over to other physical devices or locations. Thus you can enhance system availability and help lower the cost and complexity of disaster-recovery solutions.

- Increased flexibility:

  Virtualization supports the pooling of resources that can be managed centrally through an enterprise hub to better support changing business requirements dynamically.

- Enabled access through shared infrastructure:

  Virtualization provides a resilient foundation and shared infrastructure that enables better access to infrastructure and information in support of business applications and service-oriented architectures (SOA).

Companies of all sizes are aggressively adopting virtualization solutions to help in the following areas:

- Infrastructure simplification:

  Virtualization can help control infrastructure sprawl through the deployment of virtual servers and storage that run securely across a shared hardware environment. Virtualization not only helps with server consolidation, but also server containment when deploying new systems. Consolidating to a virtual infrastructure can enable you to increase server utilization rates from 5% to 15% to over 70%, thus helping improve ROI. In addition, a simplified infrastructure can help lower management costs with a common management platform and tooling.

- Rapid application deployment:

  Virtualization can help enable rapid infrastructure provisioning (in minutes instead of days). It can help developers speed application test and deployment, enhance collaboration, and improve access to the infrastructure. The ease and flexibility of creating and reconfiguring guest operating systems helps development and test environments to realize significant benefits from virtualization.

- Business resiliency:

  Virtualization can help IT managers secure and isolate application workloads and data within virtual servers and storage devices for easier replication and restoration. This added resiliency can provide IT managers with greater flexibility to maintain a highly available infrastructure while performing planned maintenance. It also helps in configuring low-cost disaster recovery solutions.

  Virtualization technologies solve many traditional backup issues, because they decouple the bindings between the operating system (with the application and data) and the underlying hardware. For example, you can have a different hardware topology in the recovery site, both in terms of the number of servers and the configuration of those servers. You can also still boot all your guests on the two different data centers.

With virtualization, you can freely mix and match technologies through common management tools for managing distributed heterogeneous resources. This added freedom offers capabilities to lower switching costs, add flexibility and freedom of choice, and mask complexity. Managing each computer or resource together virtually, instead of separately, allows for significant improvements in utilization and administrative costs.

## 2.2 Storage virtualization

The amount of data and information that is being generated by businesses continues to grow. The IT data center manager must deal with this high rate of growth and, at the same time, look for ways to reduce costs. Storage consolidation helps the data center manager deal with the rapid growth and costs concerns. Increasing the utilization of the storage hardware, similar to what was explained for the server hardware, is cost-effective and helps meet the growing demand. Storage consolidation is the allocation or provisioning of shared storage resources.

This consolidation is enabled by storage virtualization (Figure 2-1). Shared storage is connected to the servers by using Fibre Channel or IP-based networks.

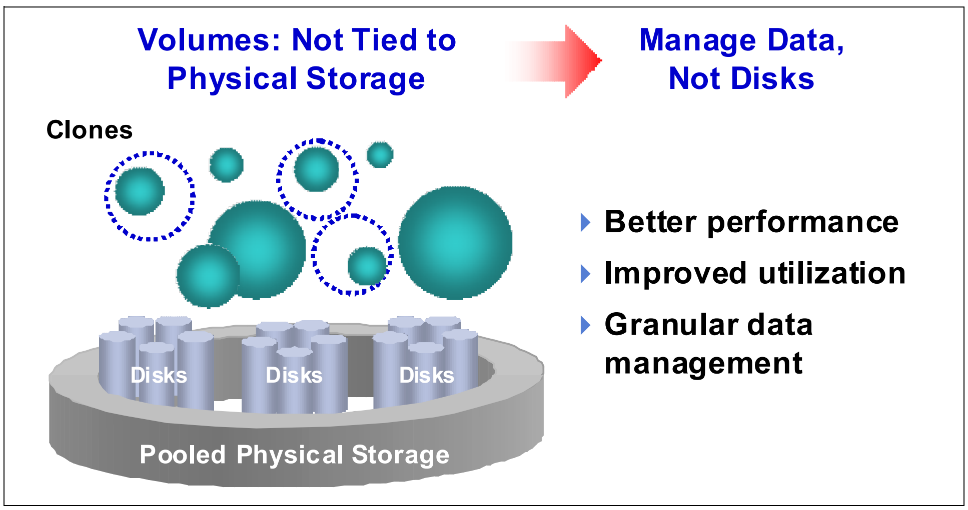



*Figure 2-1 Storage virtualization*

Storage virtualization software, which is similar in concept to server virtualization, abstracts the storage hardware volumes of data into a logical or virtual view of the volume. Using N series hardware with storage virtualization gives the data center a method to support storage provisioning, independent of the underlying storage hardware.

Storage virtualization can enable data sharing, data tiering, improved storage hardware utilization, improved availability, and disaster recovery capabilities. Storage virtualization software separates the representation of the storage to the operating system from the physical device. Utilization rates of storage are likely to be improved when moving toward network-based storage that is virtualized.

## 2.3 Network virtualization

If physical server farms are consolidated into virtual server farms, parts of the physical network can be replaced by a virtual network, saving money and reducing management complexity. Network performance and bandwidth between the servers is increased, enabling new data-intensive applications. Although network virtualization is not covered in detail in this IBM Redbooks publication, this section provides a brief overview of it. It also highlights the various technologies within the platform-specific topics.

Business-critical applications require more efficient management and use of network resources regarding performance, resource usage, people cost, availability, and security. Network virtualization includes the ability to manage and control portions of a network that can even be shared among different enterprises, as individual or virtual networks. At the same time, isolation of traffic and resource utilization is maintained.

Network virtualization includes technologies such as Virtual Private Networks (VPNs), IBM HiperSockets™, Virtual Networks, and VLANs. It also includes the ability to prioritize traffic across the network, through quality of service (QoS), to ensure the best performance for business-critical applications and processes. Instrumentation of network resources and operations, such as Simple Network Management Protocol (SNMP), can be abstracted across the server and networking devices. These technologies are key enablers for on-demand behavior.

The N series assists with this network virtualization with its ability to support multiprotocols and transports:

- Common Internet File System (CIFS)
- Network File System (NFS)
- iSCSI
- Fibre Channel Protocol (FCP)
- Fibre Channel over Ethernet (FCoE)

As illustrated in Figure 2-2, this virtualization of protocols enables consolidation of storage and reduces any connection impact to the existing network.

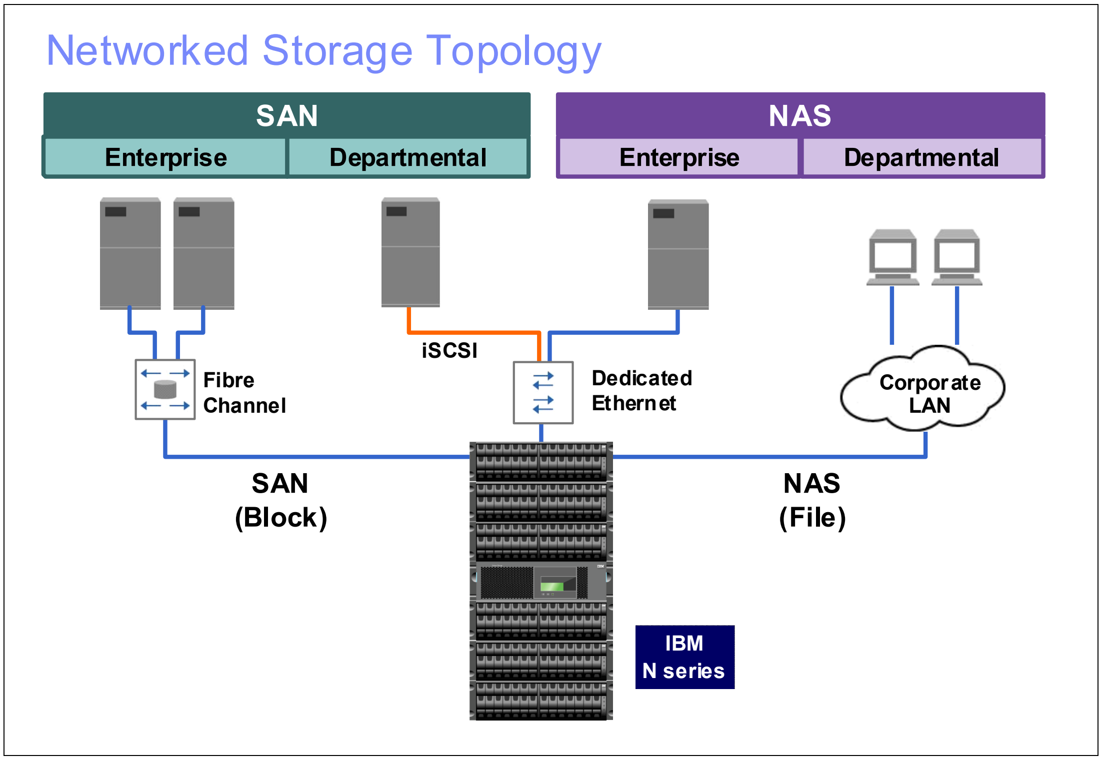



Figure 2-2 Multiprotocol N series

## 2.4 Application virtualization

Application virtualization addresses application-level workload, response time, and application isolation within a shared environment. Application virtualization complements server, storage, and network virtualization as illustrated in Figure 2-3.

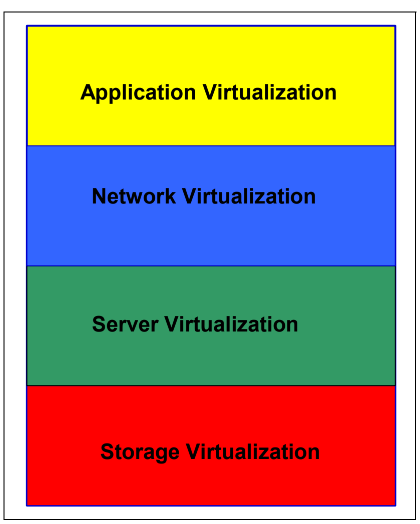



Figure 2-3 Virtualization stack

With application virtualization, businesses can push the boundaries of their IT infrastructures further for greater agility, cost savings, operational efficiency, and manageability. Also, CIOs and IT administrators can literally do more with less. With application virtualization, data centers can run applications on any application server in a common resource pool. Furthermore, administrators can deploy resources quickly and seamlessly during peak periods and in response to unforeseen demand for mission-critical applications. In addition, data administrators can achieve application response times and service levels that meet service level agreements.

## 2.5 Server virtualization

With virtualization, one computer does the job of multiple computers, by sharing the resources of a single computer across multiple environments (Figure 2-4). By using virtual servers and virtual desktops, you can host multiple operating systems and multiple applications locally and in remote locations, freeing you from physical and geographical limitations.

Server virtualization also offers energy savings and lower capital expenses because of more efficient use of your hardware resources. You also get high availability of resources, better desktop management, increased security, and improved disaster recovery processes when you build a virtual infrastructure.

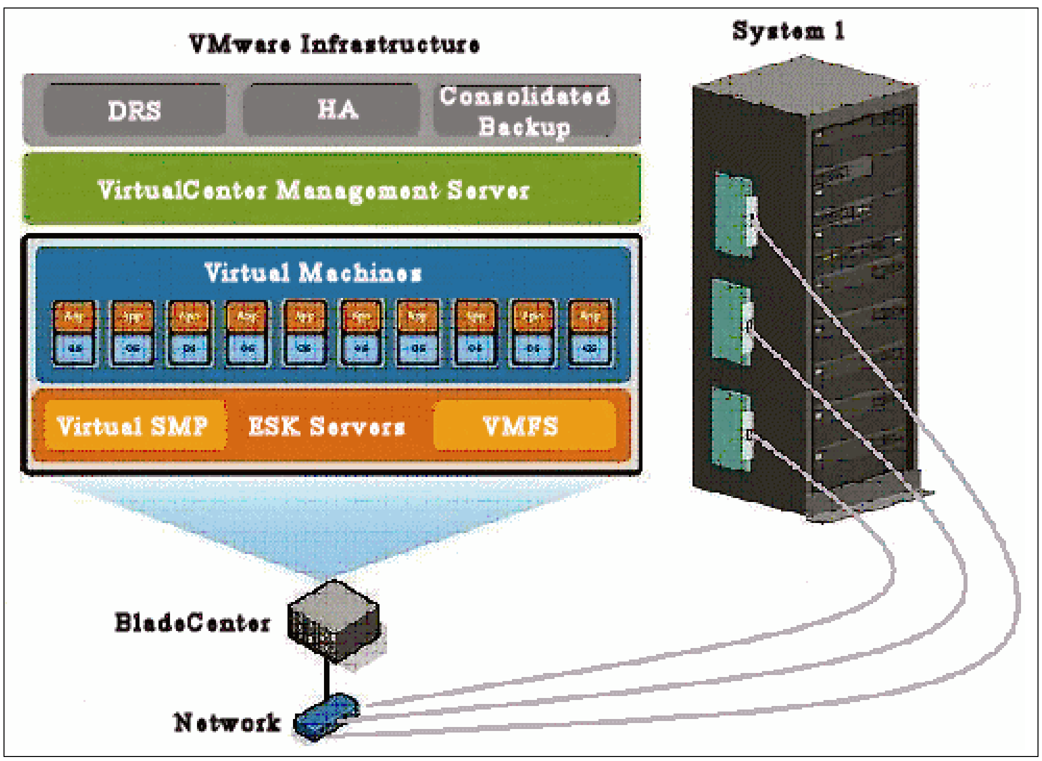



Figure 2-4 Server virtualization

The virtualization concept became more popular with the introduction of hypervisors (software responsible for the virtualization layer) in the x86 platform. However, server virtualization is not a new technology. It was first implemented more than 30 years ago by IBM as a way to logically partition mainframe computers into separate virtual machines. These partitions allowed mainframes to *multitask* (run multiple applications and processes at the same time). However, because of the high cost of the mainframes, the virtualization technology did not become popular.

The broad adoption of Microsoft Windows and the emergence of Linux as server operating systems in the 1990s established x86 servers as the industry standard. The growth in x86 server and desktop deployments introduced new IT infrastructure and operational challenges. Virtualization in the x86 platform allowed companies to centralize the management of servers and desktops, together with a reduction in cost of management.

## 2.5.1 VMware vSphere

The VMware approach to virtualization inserts a thin layer of software directly on the computer hardware (with the bare metal hypervisors as ESX and ESXi). Or it can be done on a host operating system (with the VMWare Server product). This software layer allocates hardware resources dynamically and transparently. Thus it enables multiple operating systems to run concurrently, each unaware of the others, on a single physical computer.

The VMware vSphere, combined with IBM System Storage N series storage and its storage virtualization capabilities, brings several benefits to data center management:

- Server consolidation and infrastructure optimization:

  Virtualization makes it possible to achieve higher resource utilization by pooling common infrastructure resources and breaking the “one application to one server” model.

- Physical infrastructure cost reduction:

  With virtualization, you can reduce the number of servers and related IT hardware in the data center. The benefit is reductions in real estate, power, and cooling requirements, resulting in lower IT costs.

- Improved operational flexibility and responsiveness:

  Virtualization offers a new way to manage IT infrastructure. It can help IT administrators spend less time on repetitive tasks, such as provisioning, configuration, monitoring, and maintenance.

- Increased application availability and improved business continuity:

  You can reduce planned downtime and recover quickly from unplanned outages. You have the ability to securely back up and migrate entire virtual environments with no interruption in service.

- Storage savings:

  By taking advantage of the N series thin provisioning capability, you can allocate the space of the actual used files only (see Figure 2-5).

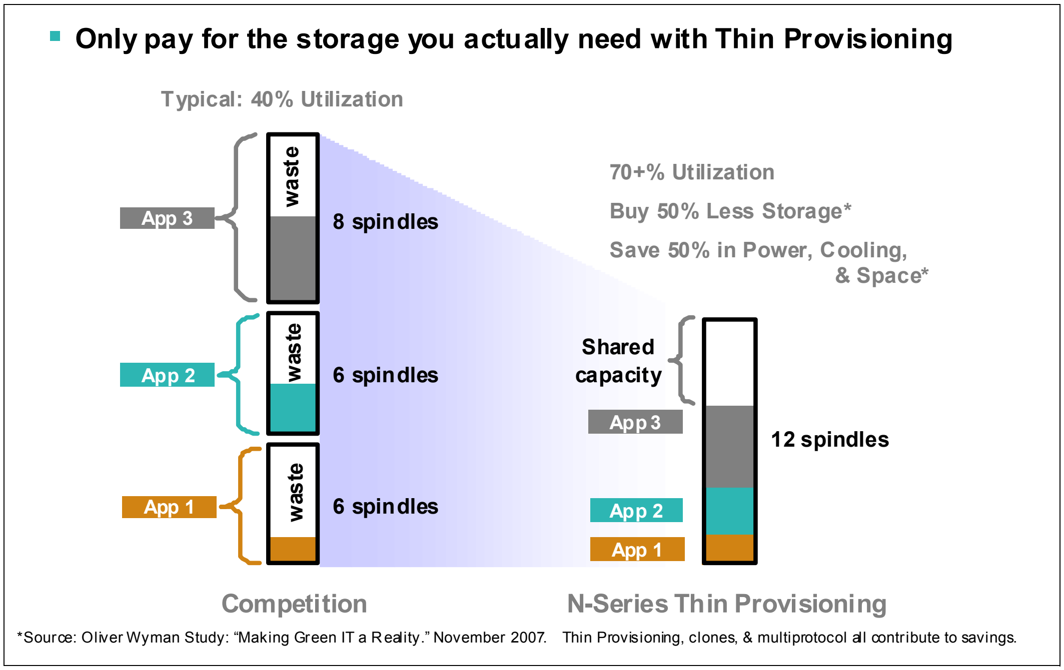



*Figure 2-5 Thin provisioning savings*

- Rapid datacenter deployment:

  With the LUN clone capability of N series system, you can quickly deploy multiple VMware hosts in the data center.

## 2.5.2 Implementation example

This section provides an example of one of several configurations that were used and implemented in the development of this Redbooks publication.

The environment has the following setup:

- Server: IBM System x3650 system
- Storage: IBM System Storage N series 6270 and an N series 5500
- iSCSI used as Storage protocol for the connection between the storage system and the server
- Ethernet switch
- Network:
  - 1-Gigabit NIC for VMware Service Console
  - 1-Gigabit NIC for VMotion
  - 1-Gigabit NIC for the virtual machines
- Virtualization software:
  - VMware ESXi 4.1
  - VMware ESX 4.1
  - VMware vCenter 4.1 Update 1

> **Network and storage redundancy:** This example does not consider redundancy for network and storage.

Figure 2-1 shows a simple diagram of the solution used.

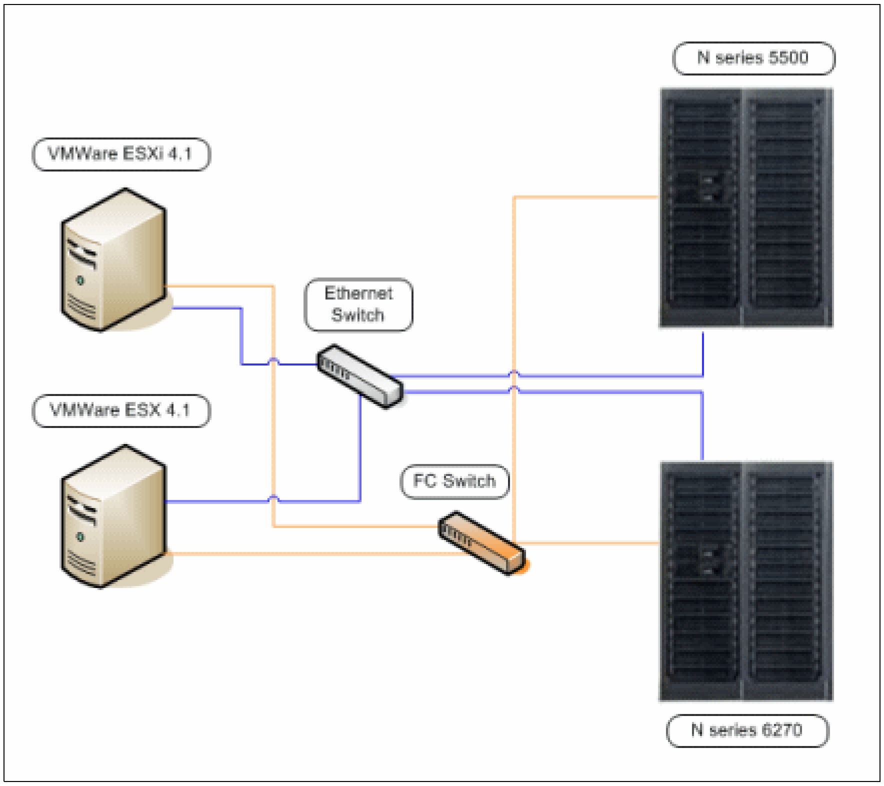



*Figure 2-6 The environment used to write this book*

3

# Benefits of N series with VMware vSphere 4.1

This chapter outlines the benefits that the IBM System Storage N series provides to VMware vSphere 4.1 environments. It includes the following topics:

- Increased protection with RAID-DP
- Cloning virtual machines
- N series LUNs for VMWare host boot
- N series LUNs for VMFS datastores
- Using N series LUNs for Raw Device Mappings
- Growing VMFS datastores
- Backup and recovery of virtual infrastructure (SnapVault, Snapshot, SnapMirror)
- Using N series deduplication with VMware

## 3.1 Increased protection with RAID-DP

In a VWware vSphere 4.x environment, the performance and availability of the storage system are important. Generally many different server systems are consolidated onto each VMware ESX host, and a failure can cause all of the machines to have an outage or data loss. RAID-DP (Figure 3-1) provides the benefit of both performance and availability without the requirement to double the physical disks. This benefit is achieved by using two dedicated parity disks. Each disk has separate parity calculations, which allows the loss of any two disks in the Redundant Array of Independent Disks (RAID) set while still providing excellent performance.

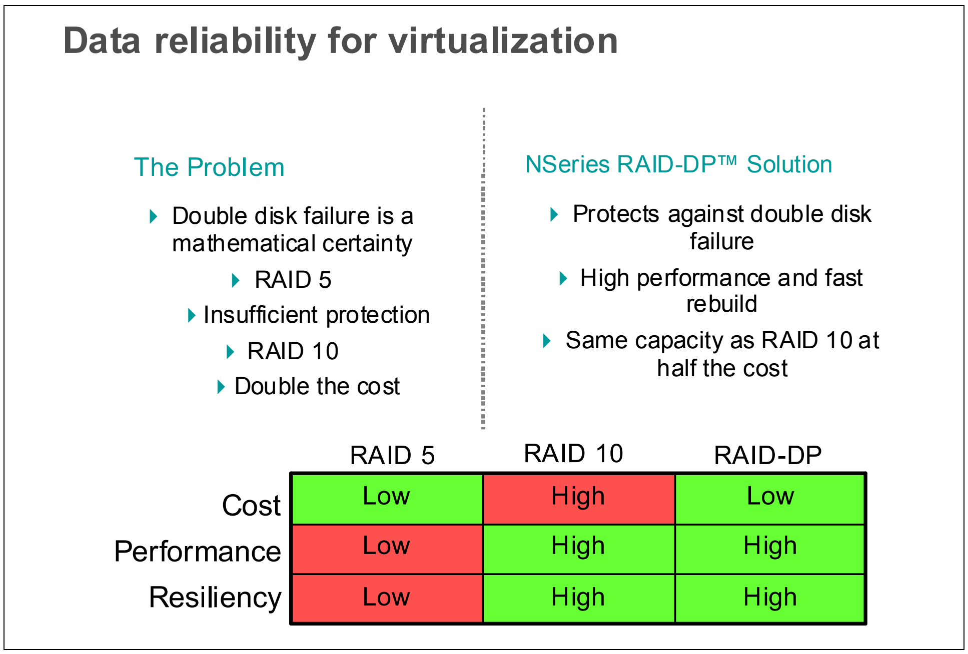



*Figure 3-1 RAID-DP*

## 3.2 Cloning virtual machines

Although you can clone guests natively with VMware, cloning from the N series provides significant storage space savings. This type of cloning is helpful when you need to test existing VMware guests. Guests can be cloned at the N series level and use little additional disk capacity due to the deduplication. We explain how this works in 3.9, “Using N series deduplication with VMware”, where VMware guest cloning doubles the required disk allocation.

## 3.3 Multiprotocol capability for storing files on iSCSI, SAN, or NFS volumes

The N series storage system provides flexibility in the method and protocol used to connect to storage. Each has advantages and disadvantages, depending on the existing solution and the VMware environment requirements.

Traditionally, most VMware scenarios use standard Fibre Channel SAN connectivity. With N series, you can keep using this method if it is already in the environment. However, fiber connectivity can be expensive if new purchases are required. As a result, more environments are now implementing network connectivity methods to storage. Such methods include iSCSI, Network File System (NFS), and Common Internet File System (CIFS), as illustrated in Figure 3-2.

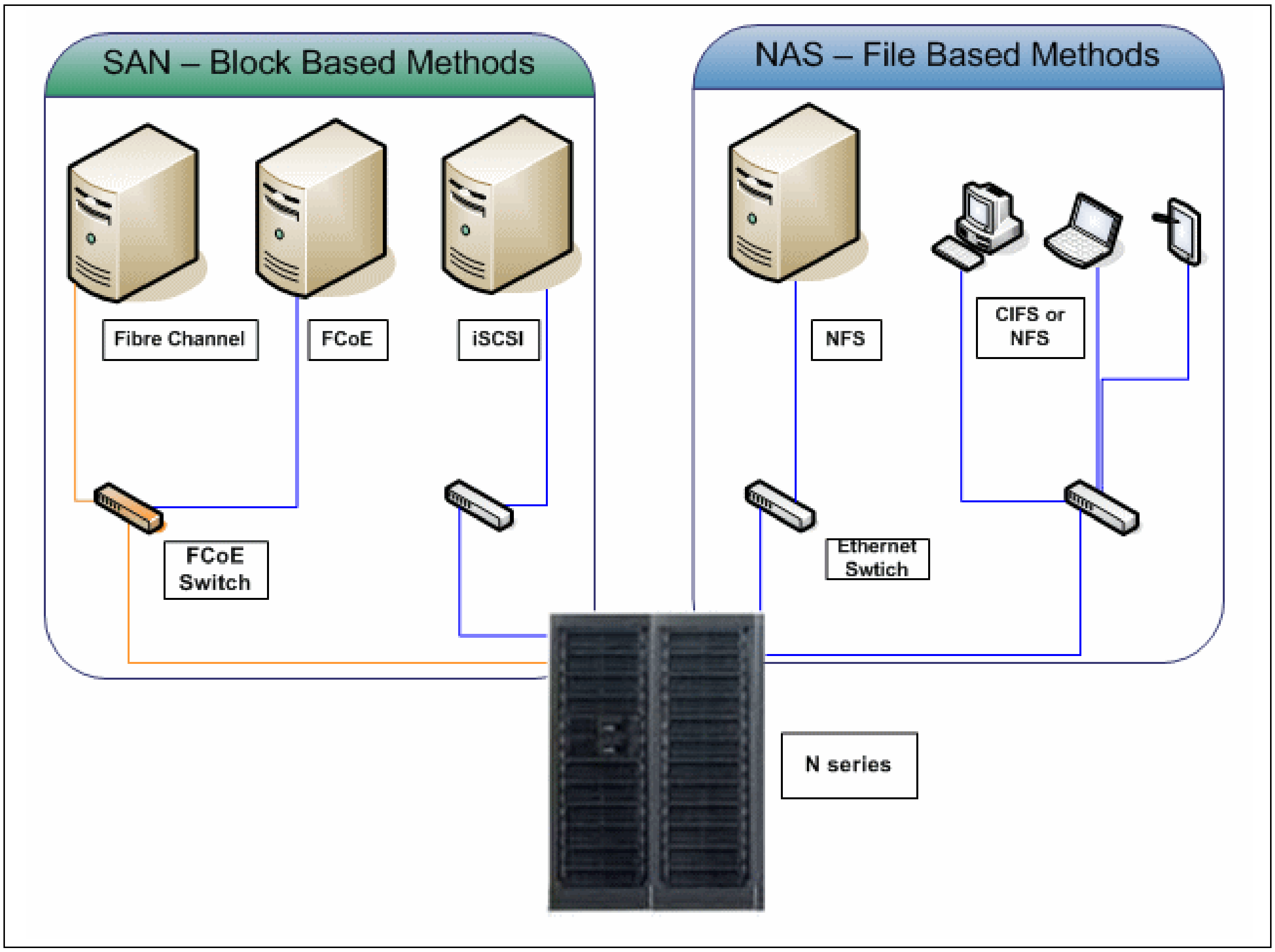



*Figure 3-2 Storage protocols used by VMWare and available on N series family*

## 3.4 N series LUNs for VMWare host boot

N series storage systems provide a set of features that make the boot from SAN reliable, secure, and cost effective. You can use these features as follows:

- With Snapshot, you can take snapshots of a logical unit number (LUN) and restore it later. You can use Snapshot restores in a case of a storage failure or for corrupted file systems if necessary to recreate the entire LUN (Figure 3-3).
- With FlexClone, you can clone a LUN and make it available to other servers. This method can be used to deploy multiple ESXi hosts. For example, you can install the ESXi operating system on a single server, then use FlexClone to make a copy of that LUN to multiple servers. This N series feature is also helpful when you want to reproduce your production environment on a test area. FlexClone functionality is shown in Figure 3-3.

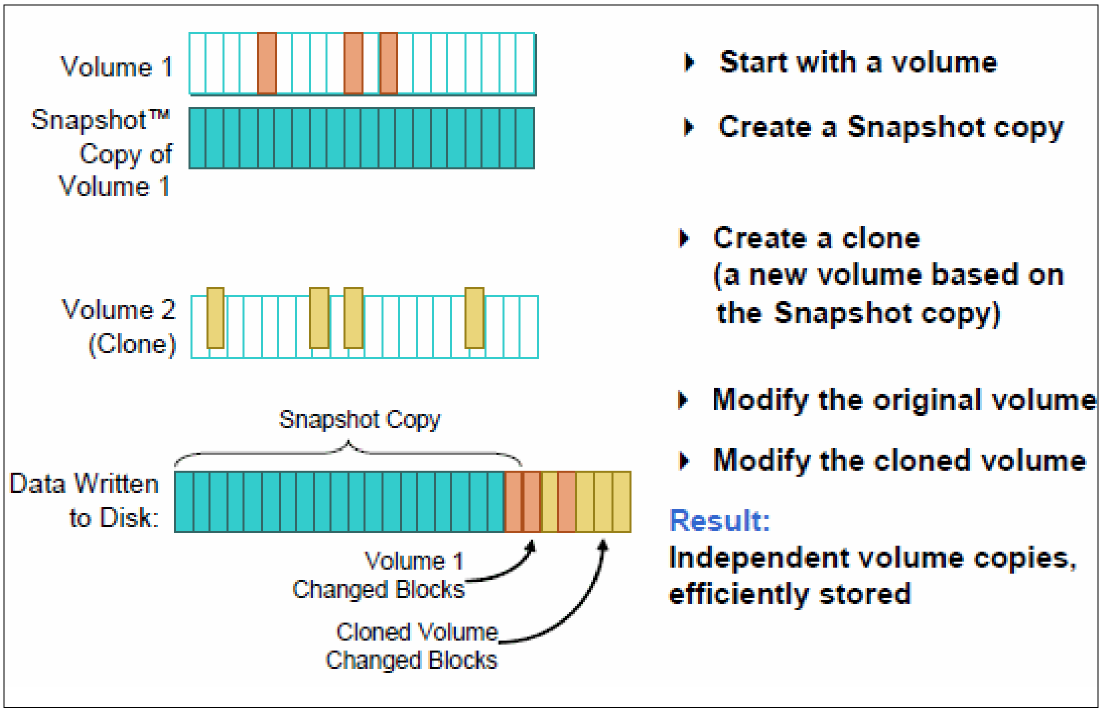



*Figure 3-3 Flexclone cloning and space savings*

**Customizing the ESXi operating system:** After using FlexClone, the ESXi operating system must to be customized to avoid IP and name conflicts with the original server from which the FlexClone was taken.

## 3.5 N series LUNs for VMFS datastores

Including many hard drives in the aggregate provides improved performance for LUNs created over them. As a best practice, ensure that each LUN is used by a single datastore, thus making them easier to manage.

Similar backup and recovery requirements provide a good criteria when deciding which servers should share the same datastores. Consider having very important servers on their own datastore, so you can take full advantage of N series advanced functionalities, which are implemented on the volume level.

## 3.6 Using N series LUNs for Raw Device Mappings

Using Raw Device Mappings (RDM) with VMware ESXi offers the following benefits:

- Mapping file references to persistent names
- Unique ID for each mapped device
- Distributed locking for raw SCSI devices
- File permission enablement
- Redo log tracking for a mapped device
- Virtual machine migration with VMotion
- Use of file system utilities
- SAN management within a virtual machine

The N series can facilitate these benefits by providing virtual LUNs though flexible volumes (Figure 3-4).

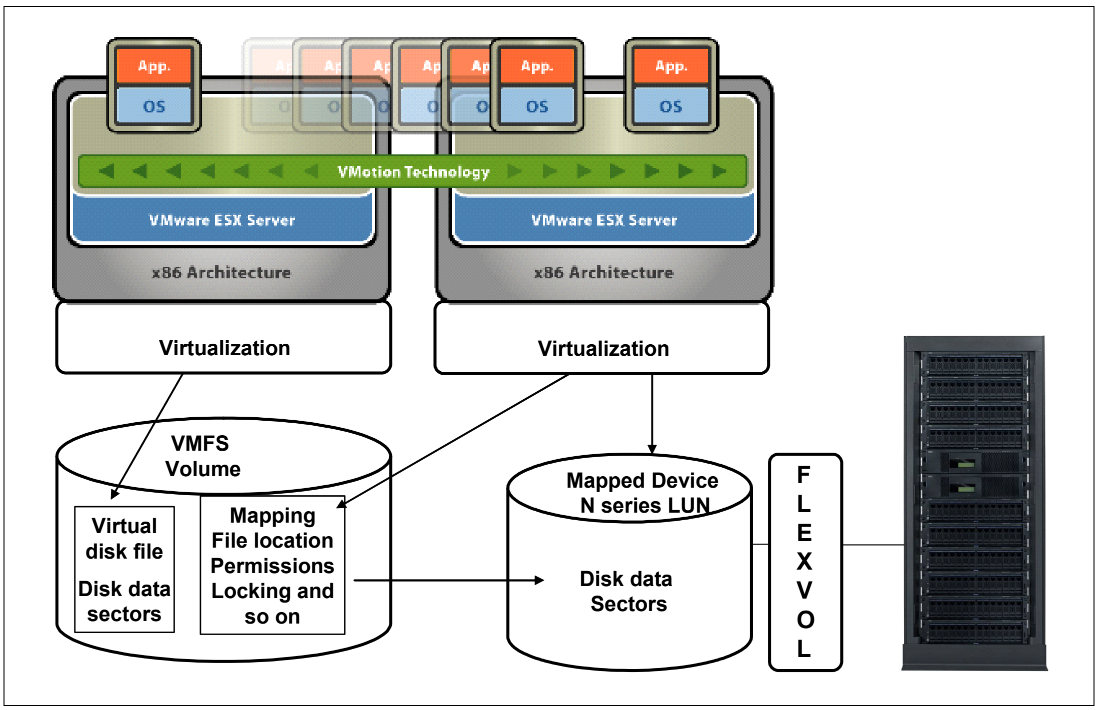



*Figure 3-4 Mapping file data*

## 3.7 Growing VMFS datastores

You can easily increase the storage for a Virtual Machine File System (VMFS) datastore by increasing the size of the N series LUN. Then you add an extent on the VMware ESX Server. However, you must complete this process only when all virtual machines stored on the datastore are shut down.

## 3.8 Backup and recovery of virtual infrastructure (SnapVault, Snapshot, SnapMirror)

The use of N series functions, such as Snapshot, allow for fast backup of a whole disk volume without using much additional disk space. The backup can then be written to tape or mirrored to auxiliary storage at the same or different location.

Recovery of a disk volume from Snapshot is fast, because the volume is quickly replaced with the Snapshot. If less data is required for restoration, such as a single file or a guest virtual machine disk (files with .vmdk extension), then the restore depends on the backup strategy:

- If *Snapshot* is used, a clone of the Snapshot can be created and just the required files can be copied back manually. For a guest, the cloned volume can be mounted by VMware and the required guests can be registered and started.
- If backup was to *tape*, a restore of the required files is performed.
- If a *mirror* exists, the required files can also be copied back manually.

It is important to note that if no other tool is implemented and a volume backup is taken, only the entire volume can be restored. To overcome that limitation, IBM offers the IBM Tivoli® Storage Manager product. This product interacts with VMWare vSphere APIs for Data Protection, formerly known as Virtual Consolidated Backup (VCB) on earlier VMWare versions. When used together, these products can restore on the image, volume, and file levels from a single backup.

For more information, see the following website:

http://www.ibm.com/developerworks/wikis/display/tivolistoragemanager/IBM+Tivoli+Storage+Manager+for+Virtual+Environments

## 3.9 Using N series deduplication with VMware

Deduplication is the concept of storing multiple instances of the same information into a single point. Then a pointer is used to refer to it on the next occurrence, so files that potentially might be stored in an environment many times are stored only once. Microsoft Exchange and Symantec Vault are commercial products known for the usage of deduplication.

N series deduplication provides Advanced Single Instance Storage (A-SIS) at the storage level, rather than the application level. Doing this significantly reduces the amount of storage that is used when the same files are stored multiple times. The deduplication process is shown in Figure 3-5.

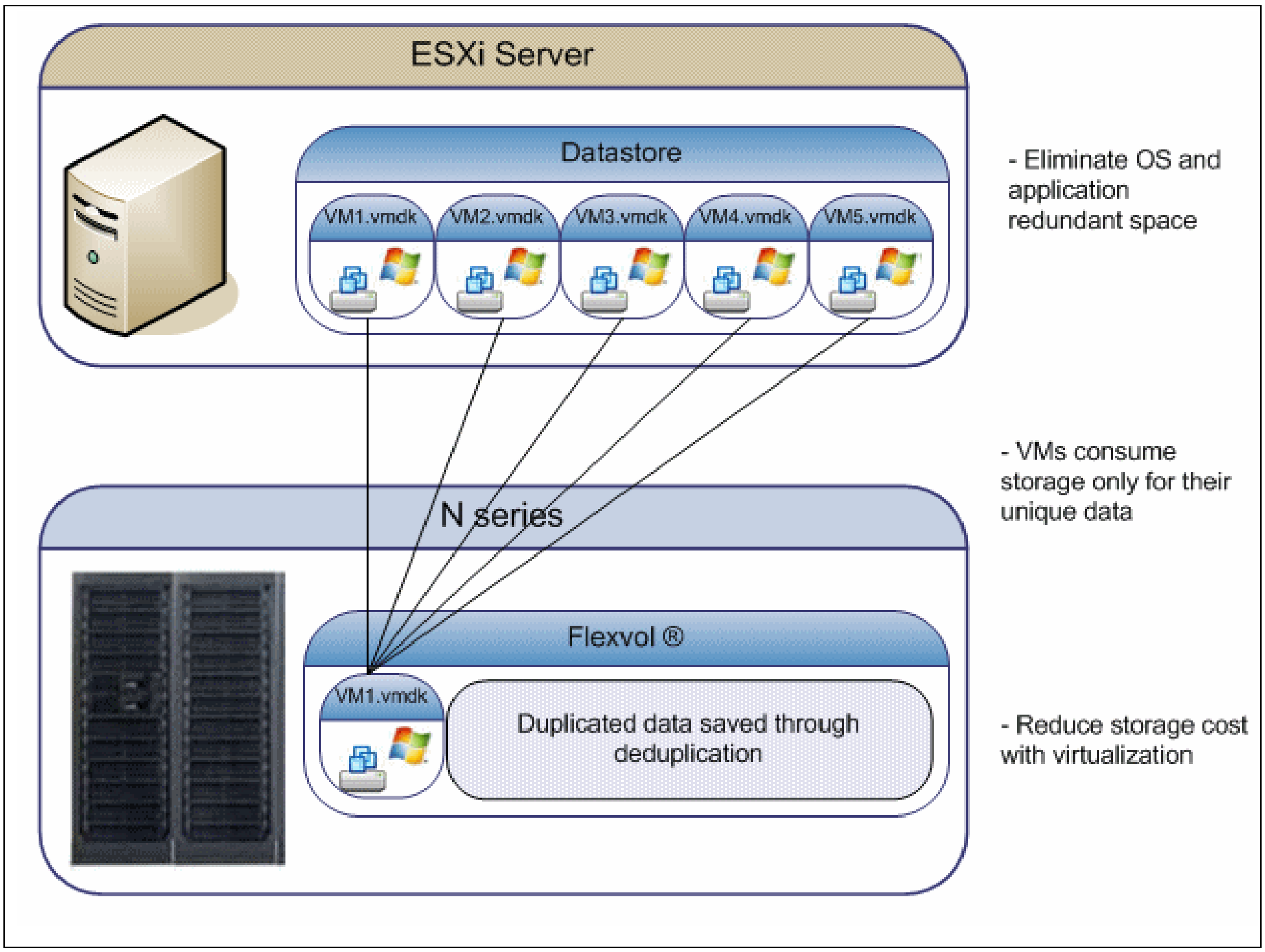



*Figure 3-5 Storage Consumption with N series A-SIS*

## 3.10 Coupling deduplication and compression

You can further increase savings by using N series deduplication and compression with the IBM Real-time Compression solution. Compression, which has been around for several years, has not met the strict IT demands for primary storage until now. To solve primary storage capacity optimization, vendors need to ensure data integrity and availability, without impacting performance or forcing IT to change their applications or process.

The IBM Real-time Compression technology meets these requirements with its Random Access Compression Engine (RACE), through an appliance called Real Time Compression Appliance (RTCA). It provides a tremendous reduction in capital and operational costs when it comes to storage management and the additional benefits of less to manage, power, and cool. Additionally, similar to server virtualization, IBM Real-time Compression fits seamlessly into your storage infrastructure. This is done without requiring changes to any processes and offering significant savings throughout the entire data life cycle.

IBM Real-time Compression provides data compression solutions for primary storage, enabling companies to dramatically increase storage efficiencies. IBM Real-time Compression provides the following benefits:

- Up to 80% of data footprint reduction.
- Resource savings. Compressing data at the origin triggers a cascading effect of multiple savings across the entire information life cycle. As less data is initially written to storage, it results in these improvements:
  - There is a reduction in storage CPU and disk utilization.
  - Effective storage cache size increases in proportion to the compression ratio and enables higher performance.
  - Snapshots, replications, and backup and restore-related operations all benefit from the data reduction and perform better.
- Transparency. No configuration changes are required on the storage, networks, or applications. The IBM Real-time Compression system is agnostic to both data types and storage systems.
- Simplicity. IBM Real-time Compression Plug and Play real-time data compression appliances are simple to deploy, with a typical installation taking no more than 30 minutes.

For more details on integration of vSphere 4.x environments with the IBM Real-time Compression Appliance (RTCA), see the IBM Redbooks publication: *Introduction to IBM Real-time Compression Appliances*, SG24-7953-01. It is located at the following website:

http://www.redbooks.ibm.com/abstracts/sg247953.html?Open

4

# Planning for an N series and VMware vSphere 4.1

This chapter explains how to plan the setup of an N series and VMware ESXi installation. It includes the following topics:

- Planning requirements
- Overview of solution sizing
- Planning for the virtualized solution
- Configuration limits and guidance
- vol options <vol-name> no_atime_update on
- Storage provisioning
- Storage connectivity
- Networking for IP storage
- Increasing storage utilization
- Snapshots
- Backup and recovery
- N series FlexShare
- Licensing

## 4.1 Planning requirements

The first step to be taken when implementing a new technology is planning. This step is often underestimated because of lack of knowledge and the non-immediate results of an unplanned system.

The aim is to have a long lasting implementation with as few problems as possible. This chapter discusses some considerations you need to keep in mind when planning your environment and the integration of its components.

### 4.1.1 Compatibility and support

The first step in ensuring the feasibility of a solution is to check its compatibility. Both hardware and software must be certified and supported to work with each other. Otherwise, you might not have support from the vendors if needed.

Because your server hardware might be from different vendors, we are providing the storage and software compatibility references.

### 4.1.2 Data ONTAP

Although Data ONTAP has supported VMware products since the introduction of the N series product line, this support is continually being enhanced. See the "IBM System Storage N series and TotalStorage NAS interoperability matrices" web page at the following address for the latest supported solutions:

http://www-03.ibm.com/systems/storage/network/interophome.html

**Access to IBM Systems support:** You must register for access to IBM Systems support applications and content. You can register at the following address:

https://www-304.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=REGS-NAS&brandind=5345868

### 4.1.3 VMware vSphere 4.1

To ensure that your overall solution is supported by VMware vSphere and IBM, see the VMware Compatibility Guide, located at the following website:

http://www.vmware.com/resources/compatibility/search.php

## 4.2 Overview of solution sizing

For your virtualized environment to deliver successful results, you must ensure that both the servers and the storage subsystems are sized appropriately. The following topics can help you to avoid overlooking items that can cause bottlenecks and that might negatively impact your environment.

Before deciding which hardware your solution is to use, monitor the systems that you intend to virtualize. Create a performance baseline wide enough to encompass both periods of low utilization and peak usage, as well as month-end closing activities. Doing this can help avoid having a distorted picture of resource utilization, which could lead to an incorrect capacity analysis and consequent inappropriate hardware acquisition.

### 4.2.1 VMware ESXi Server sizing

Virtual machines provide resources to the operating system and applications so they can perform their activities. If those resources are not enough, the requester must wait for their availability. Although virtualization is a way to share resources among different servers, it is important to have resources available at the time they are requested.

The core applications running on the servers, generally related to the company's business, are by far the most important to be measured and provided with resources. However, programs used to maintain the main ones cannot be overlooked, such as backup and antivirus, particularly when taking the consolidation approach. If you miss a program that uses 50 MB of memory, it might not impact the performance of a physical machine. But if you consolidate 20 virtual machines over a VMware ESXi server, you must add at least 1 GB of memory to your hardware needs. If those resources are not promptly made available to the secondary applications, they must compete with the primary ones, causing bottlenecks.

Here are four main resources that you need to take into account:

- Processors
- Memory
- Networking bandwidth
- I/O capabilities

Hardware shortages are often masked when the virtual machines are distributed equally among multiple VMware servers. Suppose that a physical server fails and the VMs running on that server are distributed to the remaining systems. In such a case, a small hardware shortage can become a critical business problem that manifests as poor performance.

This section provides an overview of VMware vSphere sizing. For detailed information such as sizing maximums, see the VMware support web pages:

http://www.vmware.com/pdf/vsphere4/r41/vsp_41_config_max.pdf

### 4.2.2 N series sizing

The N series product line offers plenty of options when sizing for a given solution. Whether your requirements are for a small entry level system, a medium sized system, or even a large enterprise class system, there is an N series system that can meet your needs. However, your solution must be sized to meet the demands that your applications place on it. Sizing the solution is far more important in a virtualized environment than a standard environment. This is because performance impacts affect multiple applications and lines of business.

### N series hardware

Most N series systems run all advanced functionality software that is offered in the N series product line. However, each function that an N series system must perform impacts the I/O capabilities of that device. Therefore, if your solution requires a moderate I/O rate for the applications it runs, you might want to look deeper into the overall goals of the virtualization project.

Often, virtualization projects are carried out to simplify or consolidate the environment. N series systems deliver a high performing solution for this goal, because they can displace both Network File System (NFS) and Common Internet File System (CIFS) file servers. However, this workload requires system resources and must be taken into account when deciding which N series is correct for the solution. Additionally, if the primary system must be replicated to an alternate location for backup or disaster-recovery purposes, this replication can impact the size of the N series system that is required.

Finally, local space saving functionality, such as N series deduplication, also requires system resources. The N series model chosen must be large enough to accommodate the extra processing.

After you take these considerations into account, you might need a larger system than you initially thought. Keep in mind that all of the N series systems are easy to administer and offer many virtualization enhancements that can save time and money in the end.

### N series physical drive size

With the increasing size of disk drives, it is easy to fall into the trap of sizing your storage subsystem based on the amount of storage space required. To further exacerbate this problem, N series systems run well with large drives, even with large SATA drives. However, in a virtualized environment, you must use the overall I/O per second (IOPS), MBps, or both to calculate the number of disk drives that are used.

If you do not calculate the number of disk drives, you can run into performance bottlenecks that can be easily avoided. For example, an N series system can seem to be running out of write cache when it is unable to get data to disks quickly enough because large disk drives are too few. Deciding on the number and size of disk drives to use based on the performance needs of the overall solution ensures that your applications can meet your business requirements.

### N series software

Numerous software features can address many of the diverse business needs that a company might have. Almost all of these features can be run on almost all of the N series models. However, as stated earlier, each software feature requires a slice of the system resources. Additionally, as you apply more software features to a system, the requirements and possibly limitations of the N series hardware become more important.

Therefore, engage IBM professional services to assist you with selecting the right software and the right system for all of the work that the N series system must perform.

### N series high availability

The VMware ESX Servers that you deploy must host numerous guest systems, each of which has availability requirements. Therefore, the N series system that is deployed must provide high availability. Consider a situation where none of the applications that are running are critical applications. In this case, the number of applications that might be affected by unavailable storage must encourage you to use the high availability features of the N series system for even the simplest deployment. For example, all storage systems should be clustered and using RAID-DP. For even higher availability and redundancy, we suggest using an N series MetroCluster as a foundation for VMware vSphere solutions (Figure 4-1).

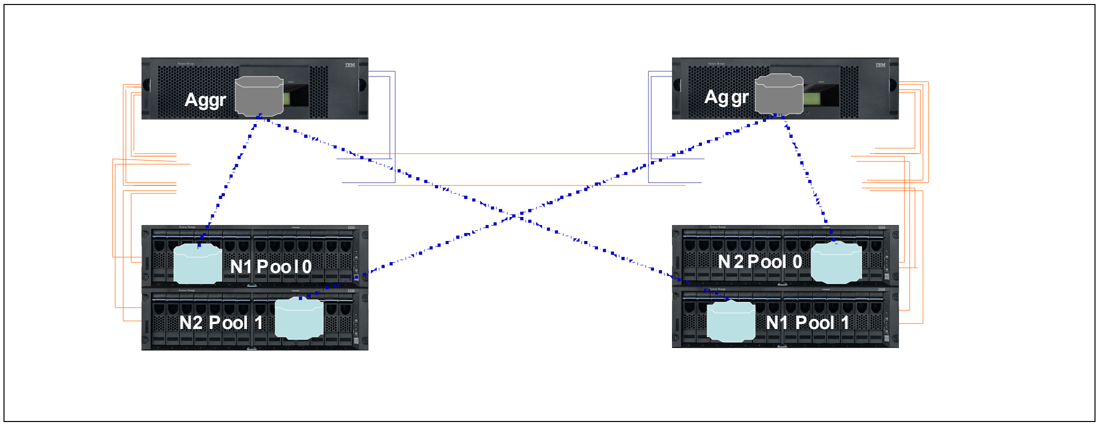



*Figure 4-1 N series MetroCluster protection*

## 4.3 Planning for the virtualized solution

Many areas of the virtualized solution require decisions to be made on how the environment is to be configured and ultimately function. This topic examines the options within each of these decision points. You must consider the ramifications of each decision based on the overall solution and the requirements that must be obtained.

**Important:** Read this chapter throughout its entirety before you finalize your decisions, because you might find restrictions or limitations that alter your choices.

### 4.3.1 Storage delivering options

There are three types of storage methods available to VMware vSphere 4.1. The following sections review each of these options and summarize the unique characteristics of each.

### VMFS datastores

VMFS datastores are logical partitions created over LUNs, provided either through Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), or iSCSI methods. They are then formatted with the Virtual Machine File System (VMFS) file system. It sends SCSI commands encapsulated on Fibre Channel or IP, for FC or iSCSI respectively. This is the most common method for deploying storage in VMware environments (see Figure 4-2).

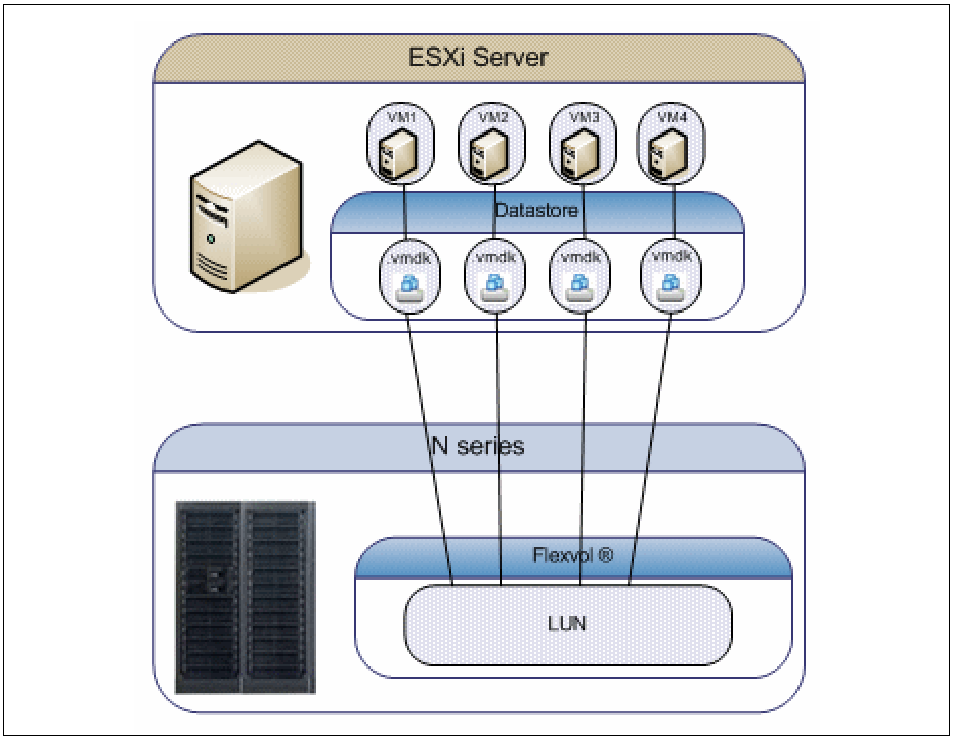



*Figure 4-2 VMFS datastore: Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), iSCSI*

The challenges associated with this storage design focus around performance scaling and monitoring. This design has a layered I/O effect where I/Os for individual guests are aggregated together as read and write requests to a shared datastore. As the number of guest machines increase on a datastore, administrators must be aware of the increase in aggregated I/O to the datastore. Individual guests that are generating higher I/O loads cannot be identified by the storage array. To identify storage bottlenecks, storage administrators must reference the VMware vCenter.

For information about accessing virtual disks stored on a VMFS using either Fibre Channel Protocol (FCP) or iSCSI, see the related VMware Guides at the following addresses:

http://www.vmware.com/pdf/vsphere4/r41/vsp_41_san_cfg.pdf
http://www.vmware.com/pdf/vsphere4/r41/vsp_41_iscsi_san_cfg.pdf

### VMFS datastores over Fibre Channel protocol

This solution comprehends the utilization of HBAs, switches, and storage devices that communicate using Fibre Channel protocol, which encapsulates the SCSI disk commands. That protocol has minimum overhead and is not routable. This solution has the following characteristics:

- Fibre Channel has the lowest latency rates, contributing to a fast connectivity.
- Multipathing must be managed carefully to avoid path thrashing when failover and failback occur.
- Data is managed from the VMWare side, commonly from VMWare vCenter.
- The storage performance is easily accessible through the Performance tab either on vCenter or directly on the host, using the Virtual Client Infrastructure.
- It has a higher cost due to the fiber components, as fiber HBAs on the servers, fiber cables and Fibre Channel Switches, also known as fabric.

### VMFS datastore over iSCSI protocol

Because Fibre Channel components can be expensive, a new solution emerged, using the existing network infrastructure existing on datacenters, based on Ethernet. In that way, you can use the common server network interfaces to connect to a storage, as the SCSI commands are encapsulated over an IP package.

The iSCSI solutions have the following characteristics:

- As they use common network components, they cost less than Fibre Channel solutions.
- Multipathing is easy to implement.
- Data is managed from the VMWare side, commonly from VMWare vCenter.
- The storage performance is easily accessible through Performance tab either on vCenter or directly on the host, using the Virtual Client Infrastructure.
- Latency is higher than using Fibre Channel due to IP encapsulation of SCSI commands.

### Raw Device Mapping over Fibre Channel

Raw Device Mapping (RDM) was introduced in VMware ESX Server V2.5. This solution has the following strengths:

- It provides high disk I/O performance.
- Easy disk performance measurement from the storage array is possible.
- It includes support for virtual machine host-based clustering, such as Microsoft Cluster Server (MSCS).
- Easy integration with features of advanced storage systems. These include N series thin provisioning, SnapRestore, FlexClone, and data deduplication, provided by the IBM System Storage N series Advanced Single Instance Storage (A-SIS)

The challenges of this solution are that VMware datacenters might have to be limited in size. This design requires an ongoing interaction between storage and VMware administration teams. Figure 4-3 shows an example of this configuration. Each virtual disk file has a direct I/O to a dedicated logical unit number (LUN). This storage model is analogous to providing SAN storage to a physical server, except for the storage controller bandwidth, which is shared. In this design, the I/O of each virtual machine is managed individually by the N series storage system.

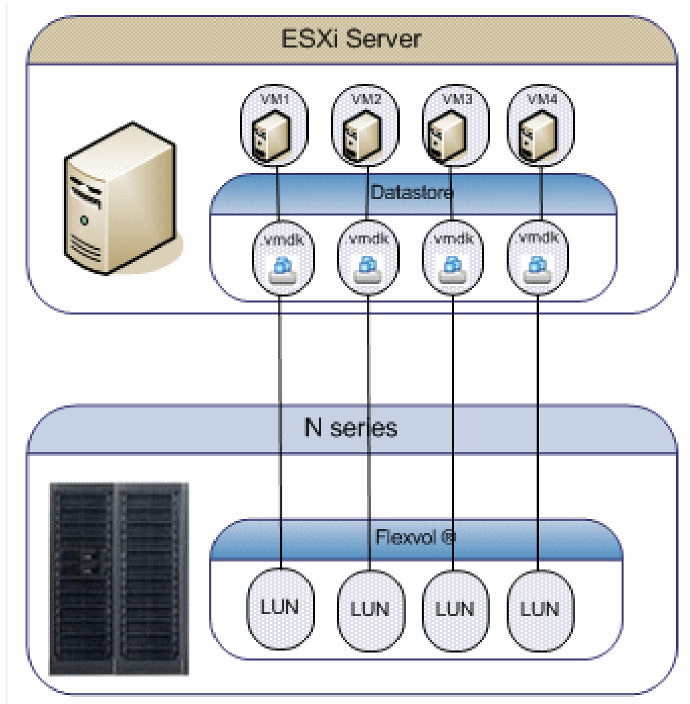



*Figure 4-3 RDM access of LUNs by guests*

For more information about RDM over Fibre Channel, see the documents available at this website:

http://www.vmware.com/pdf/vsphere4/r41/vsp_41_san_cfg.pdf

## NFS datastore

Support for storing virtual disks (.vmdk) on a Network File System (NFS) was introduced with the release of VMware ESX Server V3.0. After storage has been provisioned to the ESX Servers, the VMware administrator is free to use the storage as needed, with these benefits:

- Lower costs per port: As Ethernet is used to communicate with the storage instead of Fibre Channel, there are savings on Fibre HBAs and SAN switches. For the same reason, latency is higher comparing to FC solutions.
- Space utilization savings: VMs disks are created as thin provisioned format by default.
- Storage managed performance: Each virtual disk file has its own I/O queue directly managed by the IBM System Storage N series storage system, instead of a single queue management offered by FC or iSCSI VMFS datastores.
- NFS is the only format both compatible with VMware and IBM Real Time Compression Appliance (RTCA).
- Space management: NFS datastores are easier to manage, as their expansion occurs automatically as soon as you extend the NFS exports on the storage side.

NFS datastores are easy to integrate with data management and storage virtualization features provided by advanced storage systems. These include N series data deduplication, array-based thin provisioning, and SnapRestore. In the NFS datastore configuration shown in Figure 4-4, the storage layout looks similar to a VMFS datastore.

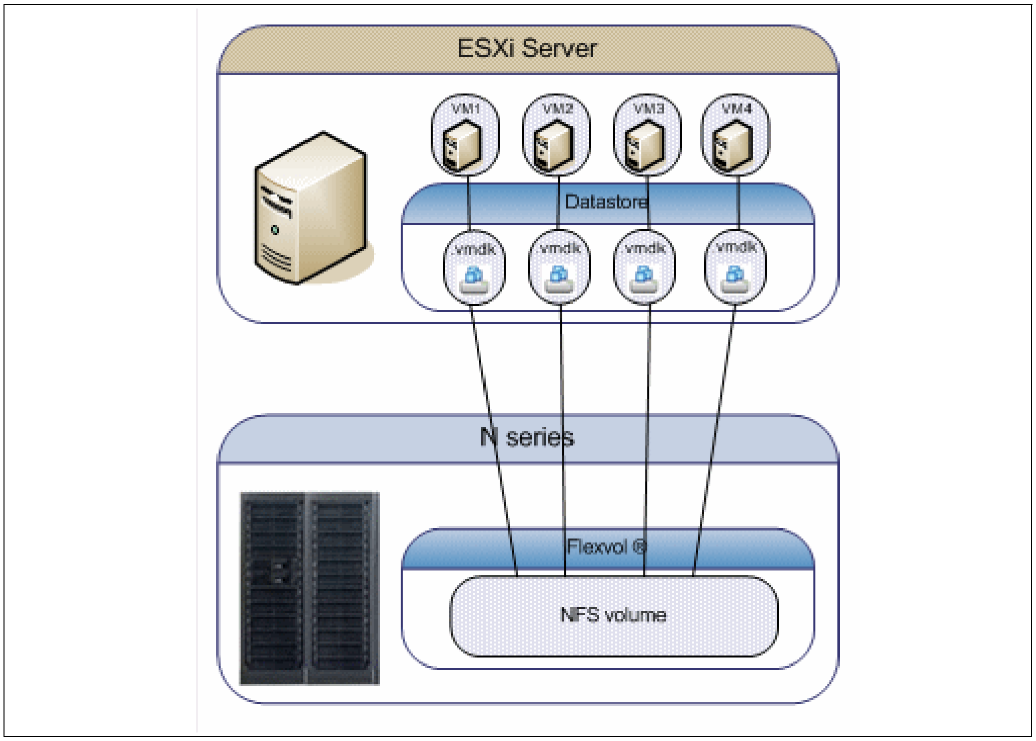



*Figure 4-4 NFS accessed datastore*

**Important:** Whenever using thin provisioned disks, carefully watch the space available on the NFS volume, as it can grow without any previous notice. If the used space exceeds the available space, all the virtual machines hosted on that volume might crash.

There are some drawbacks when using NFS that are important to keep in mind:

- Because sharing disks is not possible as in RDMs, you cannot create Microsoft Clusters over an NFS datastore.
- ESXi version 4.1 does not support hardware acceleration with NAS storage devices.

For more information about storing .vmdk files on NFS, see the *VMware ESXi Configuration Guide* at the following website:

http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esxi_server_config.pdf

## 4.3.2 N series storage configuration

This section provides information about the configuration settings for the N series base hardware and its software features.

### RAID data protection

When focusing on storage availability, many levels of redundancy are available for deployments. Examples include purchasing physical servers with multiple storage host bus adapters (HBAs) and deploying redundant storage networking and network paths to use storage arrays with redundant controllers. If you have deployed a storage design that meets all of the criteria, you might think that you have eliminated all single points of failure. Actually, data protection requirements in a virtual infrastructure are even greater than on a traditional physical server infrastructure. Data protection has become a paramount feature of shared storage devices.

RAID-DP in Data ONTAP is an advanced RAID technology that is provided as the default RAID level on all IBM System Storage N series storage systems. RAID-DP provides protection from the simultaneous loss of two drives in a single RAID group. RAID-DP is economical to deploy, because the impact with the default RAID group size is a mere 12.5%. This level of resiliency and storage efficiency makes data residing on RAID-DP safer than data stored on RAID 5 and more cost effective than RAID 10. Use RAID-DP on all RAID groups that store VMware data.

### Aggregates

An aggregate is the virtualization layer of Data ONTAP that abstracts physical disks from logical data sets, which are referred to as *flexible volumes*. Aggregates provide a means where the total IOPS available to all of the physical disks is pooled as a resource. This design is better suited to meet the needs of an unpredictable and mixed workload.

Whenever possible, use a small aggregate as the root aggregate, which stores the files that are required for running and providing GUI management tools for the N series storage system. Place the remaining storage in a small number of large aggregates.

Because the overall disk I/O from the VMware Virtual Infrastructure 3 environment is traditionally random by nature, this storage design ensures optimal performance, because a large number of physical spindles are available to service I/O requests. On smaller N series storage systems, it might not be practical to have more than a single aggregate because of a restricted number of disk drives on the system. In these cases, it is acceptable to have only a single aggregate.

### Flexible volumes

Flexible volumes (Figure 4-5) contain either LUNs or virtual disk files that are accessed by hosts. Use a one-to-one (1:1) alignment of VMware Virtual Infrastructure three datastores to flexible volumes. This design provides an easy means to help you understand the VMware ESX Server data layout when viewing the storage configuration from the N series storage system. This mapping model also provides an easy means to implement Snapshot backups or SnapMirror replication policies at the datastore level. This is because Data ONTAP implements these storage-side features at the flexible volume level.

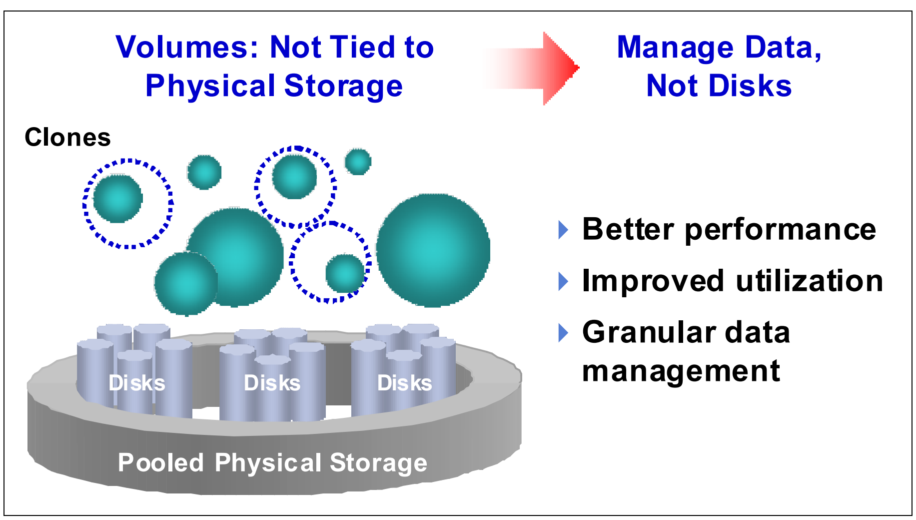



*Figure 4-5 Flexible volumes*

### LUNs

Logic Unit Numbers (LUNs) are units of storage provisioned from the N series storage system directly to the host systems. LUNs can be accessed by the hosts in two ways. The first and most common method is used for storage of virtual disks for multiple guests. This type of usage is referred to as a VMFS LUN. The second method is a Raw Device Mapping (RDM). With an RDM, the LUN is accessed by the host, which in turn passes access directly to a guest. The guest then uses its native file system, such as NTFS or EXT3.

### Storage naming conventions

With N series storage systems, you can use custom or canonical naming conventions. In a well-planned virtual infrastructure implementation, a descriptive naming convention aids identification and mapping through the multiple layers of virtualization from storage to the guest machines. A simple and efficient naming convention also facilitates configuration of replication and disaster recovery processes. Consider these naming suggestions:

- FlexVol name: The name matches the datastore name or a combination of the datastore name and the replication policy. Examples are Datastore1 or Datastore1_4hr_mirror.
- LUN name for VMFS datastores: The name must match the name of the datastore.
- LUN name for RDMs: The LUN name must have the host name and the volume name of the guest. For example, for a Windows guest, consider hostname_c_drive.lun, or for a Linux guest, consider hostname_root.lun.

# 4.4 Configuration limits and guidance

When sizing storage, be aware of the limits and guidance described in this topic.

## 4.4.1 N series volume options

Configure N series flexible volumes with snap reserve set to 0 and the default Snapshot schedule disabled. All N series Snapshot copies must be coordinated with the hosts to ensure data consistency. To set the volume options for Snapshot copies to the preferred settings, perform the following steps on the N series system console:

1. Log in to the N series console.
2. Set the volume Snapshot schedule:

   ```
   snap sched <vol-name> 0 0 0
   ```

3. Set the volume Snapshot reserve:

   ```
   snap reserve <vol-name> 0
   ```

## 4.4.2 RDMs and VMFS datastores

VMware vSphere 4.1 hosts are limited to a total of 256 LUNs. Take this limitation into consideration when planning the number of VMFS Datastores and RDM and if you are planning to have a number of Microsoft Clusters running on the environment. For example, if you have 20 MS clusters and each of them has 5 RDM disks, then 100 LUNs are needed. Therefore, you have 156 LUNs remaining to create your datastores.

Remember that RDMs store only the data disk, so you must plan the usage of a VFMS datastore to store virtual machine configuration files. The VMDK definition file associated with RDMs is reported to be the same size as the LUN, which is the default behavior within vCenter. The actual VMDK definition file only consumes a few MB of disk storage (typically 1–8 MB, which is the block size formatted with VMFS).

### 4.4.3 LUN sizing for VMFS datastores

VMFS datastores are the simplest method of provisioning storage. However, you must balance the number of datastores to be managed against the possibility of overloading large datastores with too many guests. Such an overload might cause low performance due the high combined I/O.

VMware provides Storage vMotion as a means to redistribute guest disks to alternative datastores without disruption. With large VMFS datastores, the means to reclaim the provisioned yet unused storage after a guest has migrated to an alternative datastore is reduced. thin provisioning is a way to reclaim that space, but it has to be used when the disks are created, as there is no way to turn a thick disk into a thin provisioned one.

A commonly deployed size of LUNs for a VMFS datastore is 300 GB to 500 GB. The maximum supported LUN size is 2 TB minus 512 bytes. A datastore can contain up to 32 LUNs (called extents), resulting in a 64 TB datastore.

For more information, see the following documents, *Fibre Channel SAN Configuration Guide* and *iSCSI SAN Configuration*, available at this website:

http://www.vmware.com/support/pubs/vs_pages/vsp_pubs_esxi41_i_vc41.html

## 4.5 Storage connectivity

This topic explains the available storage options and reviews the settings that are specific to each technology.

Each VMware ESXi Server must have at least two paths available to the storage in order to ensure resiliency. Those paths can be Fibre Channel HBAs or two NIC connecting to an NFS or iSCSI storage. The iSCSI connections can be software-based or hardware-based.

### 4.5.1 Fibre Channel connectivity

You might notice that the Fibre Channel service is the only storage protocol that is running by default on the VMware ESXi.

#### Fibre Channel multipathing

For storage administrators that have *Active-Active* arrays using Fibre Channel, VMware has an exciting new feature on the new version of its operating system.

Load balance can be divided into multiple paths at the same time, using ALUA specification, which was available on the previous versions of ESX, but was not supported at that time.

> **Important:** Do not use ALUA on Active-Passive Arrays.

VMware ESXi 4.1 supports officially ALUA as multipath policy, which is implemented by selecting Round Robin as the Storage Array Type, as shown in Figure 4-6.

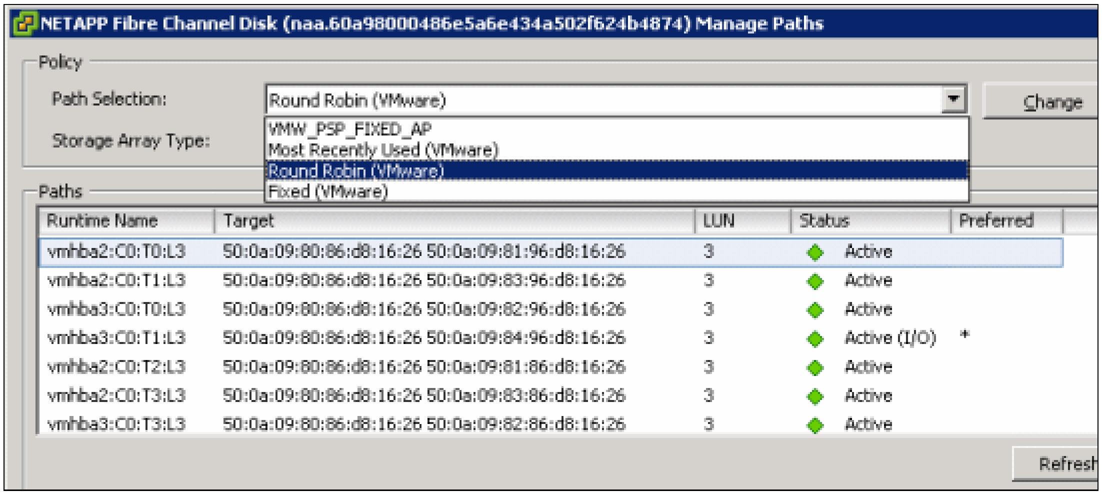


*Figure 4-6 Configuring VMware ESX as Round Robin*

Clustered N series storage systems have an option known as *cfmode*, which controls the behavior of the Fibre Channel ports of a system if a cluster failover occurs. If you are deploying a clustered solution that provides storage for VMware, ensure that cfmode is set to either Standby or Single System Image. Standby mode supports VMware, Windows, Linux, and Solaris FCP hosts. Single System Image supports all FCP hosts.

For a complete list of supported VMware ESX Server FCP configurations, see the *IBM System Storage N series SAN Interoperability Matrix for FC, iSCSI, Switch, Antivirus, and UPS* at the following website:

ftp://service.boulder.ibm.com/storage/nas/nseries/nseries_fc_san_av_ups.xls

> **Access to IBM Systems support:** You must register for access to IBM Systems support applications and content. You can register at the following address:
>
> https://www-304.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=REGS-NAS&brandind=5345868

To verify the current cfmode, follow these steps:

1. Connect to the N series system console.
2. Enter **`fcp show cfmode`**.
3. If cfmode must be changed, enter **`fcp set cfmode`** ***<mode type>***.

Standby cfmode might require more N series Fibre Channel ports and switch ports because multipathing failover is handled by the N series system and is implemented with active and standby ports. A single system image might require fewer N series Fibre Channel ports and switch ports, but additional multipathing configuration is required on the VMware ESX Server.

For more information about the different cfmodes available and the impact of changing a cfmode, see the *Data ONTAP 7.3.x Block Access Management Guide for iSCSI and FCP* at this website:

http://www.ibm.com/storage/support/nas/

See the previous note box about access to IBM Systems support application and content.

If you have implemented Single System Image cfmode, you might want to configure multipathing on the server side also. This way, you can enforce the path to be used when accessing a given LUN. Here is the procedure to change the preferred path:

1. Open vCenter.
2. Select a host.
3. Select a datastore:
   a. In the right pane, select the **Configuration** tab.
   b. In the Hardware pane on the right, select **Storage**.
   c. In the Storage box, highlight the datastore and select the **Properties** link.
4. In the Properties dialog box, click the **Manage Paths** button (Figure 4-7).

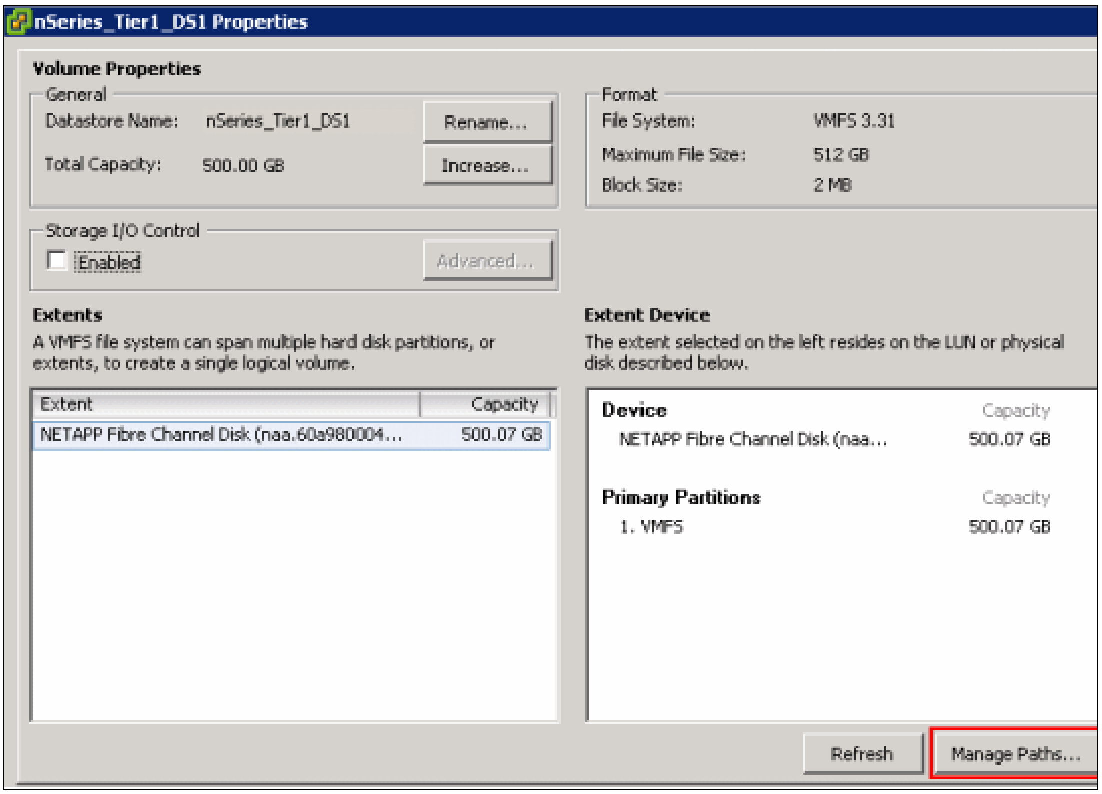



*Figure 4-7 Managing Fibre Channel Paths*

5. Identify the path you want to set as the primary path, right-click it, and click the **Preferred** button as shown in Figure 4-8.

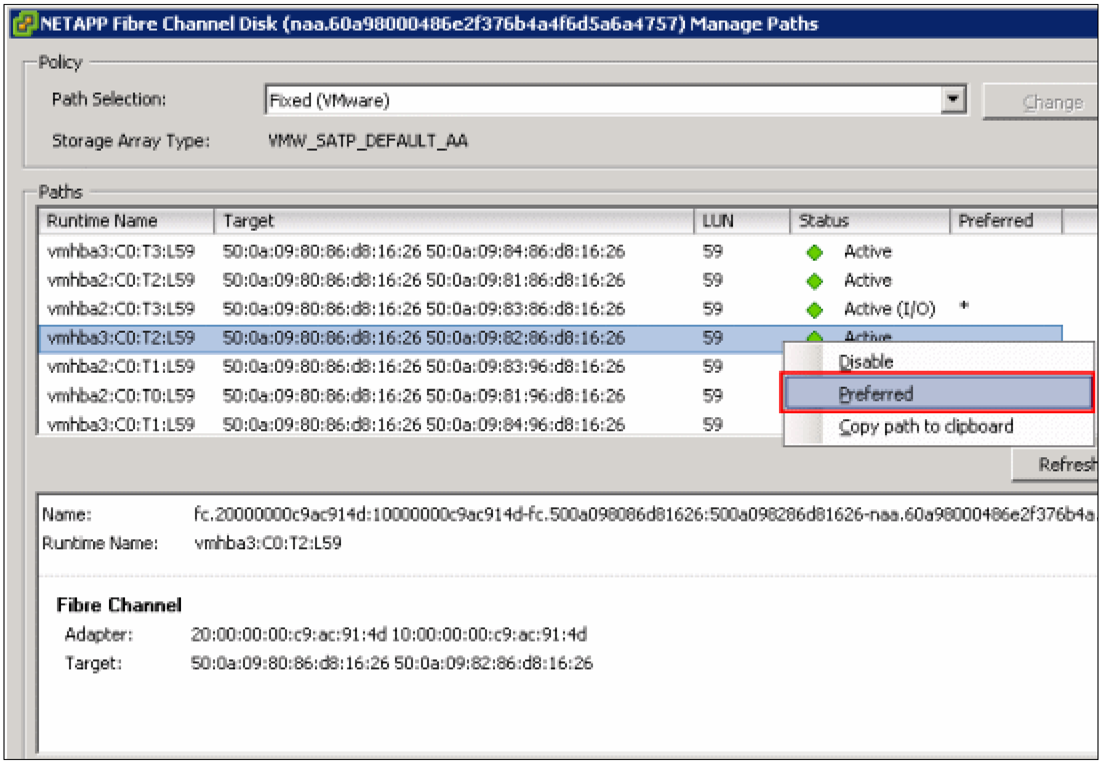



*Figure 4-8 Changing the Preferred path*

### Multipathing with N series FCP ESX Host Utilities for Native OS

IBM provides a utility for simplifying the management of VMware ESX Server nodes on Fibre Channel SAN. This utility is a collection of scripts and executable files referred to as the *FCP ESX Host Utilities for Native OS* (or simply Host Utilities).

One of the components of the Host Utilities is the **config_mpath** script. This script reduces the administrative impact of managing SAN LUN paths. The **config_mpath** script can determine the desired primary paths to each of the SAN LUNs on the ESX Server and then set the preferred path for each LUN to use one of the primary paths.

Multipathing configuration for large numbers of LUNs can be completed quickly and easily by running the **config_mpath** script once on each VMware ESX Server in the data center. If changes are made to the storage configuration, the script is run an additional time to update multipathing configuration based on the changes to the environment.

The FCP ESX Host Utilities for Native OS also has the following notable components:

- The **config_hba** script, which sets the HBA timeout settings and other system tunables required by the N series storage device
- A collection of scripts used for gathering system configuration information in the event of a support issue

For more information about the FCP ESX Host Utilities for Native OS, see the following web page:

https://www-304.ibm.com/systems/support/myview/supportsite.wss/supportresources?brandind=5000029&familyind=5329809&taskind=7

**Access to IBM Systems support:** You must register for access to IBM Systems support applications and content. You can register at the following address:

https://www-304.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=REGS-NAS&brandind=5345868

## 4.5.2 IP SAN connectivity through iSCSI

This section discusses connectivity through the iSCSI protocol.

### iSCSI overview

The iSCSI protocol is used to transfer storage commands between the storage system and servers through a TCP/IP network. This way, administrators can take advantage of their existing TCP/IP infrastructure for storage traffic. The iSCSI protocol has several key benefits. For example, it is rapid and easy to deploy compared to a traditional FCP implementation. And because it is a low-cost solution, the iSCSI protocol can run over the existing TCP/IP network. Also, it does not require any special hardware to be added to the infrastructure.

### iSCSI structure

The iSCSI protocol consists of *initiators* and *targets*. The initiators are the devices that provide access to the storage system using the iSCSI protocol. They are normally servers. The targets are the storage systems that provide the data.

To make the connection between the initiators and targets, the iSCSI protocol uses iSCSI Qualified Name (IQN) name resolution. The IQN is a global and unique name that is used by the iSCSI devices to provide iSCSI name resolution. IQNs do not change when the Ethernet adapters or IP addresses change. This provides more flexibility for the environment. Therefore, if an infrastructure change occurs, the iSCSI connections do not need to be rebuilt. The following example shows an IQN:

```
iqn.1998-01.com.vmware:server300b-6916e313
```

### iSCSI initiators

The iSCSI protocol can be a software initiator or hardware initiator:

**Software initiator** Uses codes to promote an iSCSI connection to the storage system. Normally, the software initiator is a separate program that is installed in the operating system, or in some cases, it comes built into the kernel. It does not require any additional or special hardware. It is not possible to implement boot from SAN using iSCSI software initiators.

**Hardware initiator** Uses a dedicated iSCSI HBA to establish communication with the target system. By using this type of iSCSI initiator, you can take advantage of using boot from SAN because the communication can be initiated by the firmware of the iSCSI HBA.

### iSCSI security

The most recent version of the iSCSI protocol supports both Encryption through IPSec and IKE, and Authentication through a variety of methods. These include Kerberos 5.1, Secure Remote Password (SRP), Simple Public Key Mechanism (SPKM) and CHAP (the default).

For performance reasons, separate iSCSI traffic from other IP network traffic by implementing a different physical network from the one used for VMotion or guest traffic. To enable iSCSI connectivity, it is mandatory to create a portgroup named *VMkernel port* on the virtual switch that connects to the iSCSI Storage, also known as iSCSI target.

**Portgroups:** For ESX and ESXi 3.5, a Service Console portgroup is also required to exist on the same virtual switch as the VMkernel portgroup.

A resilient network solution can be implemented in the way shown in Figure 4-9.

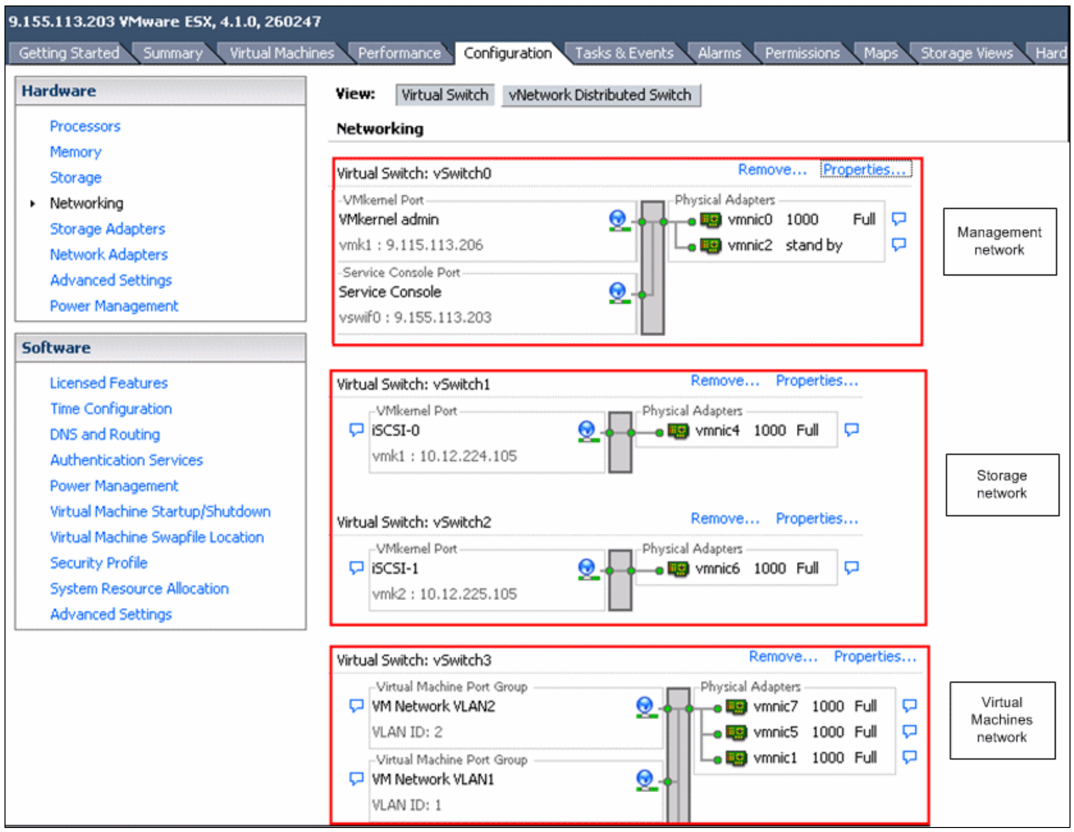



*Figure 4-9 A redundant network configuration for iSCSI or NFS file systems*

The VMkernel portgroup requires its own IP address. For more information about how to create a VMkernel portgroup,

IBM offers an iSCSI target host adapter for N series systems. Using this adapter can provide additional scalability of the N series storage system by reducing the CPU load of iSCSI transactions. An alternative to the iSCSI target host adapter is to use TOE-enabled network interface card (NICs) for iSCSI traffic. Although the iSCSI target host adapters provide the greatest performance and system scalability, they require additional NICs to be used to support all other IP operations and protocols. TOE-enabled NICs handle all IP traffic similar to a traditional NIC, in addition to the iSCSI traffic.

IBM offers iSCSI HBAs for use with iSCSI implementations. For larger deployments, scalability benefits can be realized in storage performance by implementing iSCSI HBAs. This statement is neither a requirement nor a recommendation, but rather a consideration when designing dense storage solutions. The benefits of iSCSI HBAs are best realized on N series systems. The reason is because the storage arrays have a higher aggregated I/O load than the storage array of any individual VMware ESX hosts.

### 4.5.3 NFS connectivity

When you are using NFS connectivity for storage, separate the NFS traffic from other IP network traffic. You can do this by implementing a separate network or VLAN than the one used for VMotion or guests. To enable NFS connectivity, a *VMkernel port* is also required.

IBM offers TOE-enabled NICs for serving IP traffic, including NFS. For larger deployments, scalability benefits can be realized in storage performance by implementing TOE-enabled NICs. This statement is neither a requirement nor a recommendation, but rather a consideration when designing dense storage solutions. The benefits of TOE-enabled NICs are better realized on N series systems.

## 4.6 Networking for IP storage

Use dedicated physical resources for storage traffic whenever possible. With IP storage networks, you can achieve this setup with separate physical switches or a dedicated storage VLAN on an existing switch infrastructure.

### 4.6.1 Design principles

Whenever possible, design your storage network with the following principles in mind:

- Be redundant across switches in a multiswitch environment.
- Use as many available physical paths as possible.
- Be scalable across multiple physical interfaces.

#### 10 Gb Ethernet

VMware ESX Server V3.5 introduced support for 10 Gb Ethernet. See the *VMware ESX Server I/O Compatibility Guide* at the following web page to verify support for your hardware:

http://www.vmware.com/pdf/vi35_io_guide.pdf

#### VLANs

By segmenting network traffic with VLANs, interfaces can either be dedicated to a single VLAN or they can support multiple VLANs with VLAN tagging. Use tagging interfaces into multiple VLANs (to use them for both virtual machine and storage traffic) only if enough interfaces are not available to separate traffic. (Some servers and storage controllers have a limited number of network interfaces.) If you are using multiple VLANs over the same interface, ensure that sufficient throughput can be provided for all traffic.

### N series virtual interfaces

A virtual network interface is a mechanism that supports the aggregation of network interfaces into one logical interface unit. When created, a virtual interface (VIF) is indistinguishable from a physical network interface. VIFs are used to provide fault tolerance for the network connection and, in some cases, higher throughput to the storage device.

Multimode VIFs are partly compliant with IEEE 802.3ad. In a multimode VIF, all of the physical connections in the VIF are simultaneously active and can carry traffic. This mode requires that all the interfaces are connected to a switch that supports trunking or aggregation over multiple port connections. The switch must be configured to reflect the concept that all the port connections share a common MAC address and are part of a single logical interface.

In a single-mode VIF, only one of the physical connections is active at a time. If the storage controller detects a fault in the active connection, a standby connection is activated. No configuration is necessary on the switch to use a single-mode VIF, and the physical interfaces that make up the VIF do not have to connect to the same switch. IP load balancing is not supported on single-mode VIFs.

It is also possible to create second-level single or multimode VIFs. By using second-level VIFs, you can take advantage of both the link aggregation features of a multimode VIF and the failover capability of a single-mode VIF. In this configuration, two multimode VIFs are created, each one to a different switch. A single-mode VIF is then created, which consists of the two multimode VIFs. In normal operation, traffic only flows over one of the multimode VIFs. However, in the event of an interface or switch failure, the storage controller moves the network traffic to the other multimode VIF.

## 4.6.2 Network design for storage on VMware vSphere 4.1

To have a solid base of the storage network configuration for your installation, see the *iSCSI SAN Configuration Guide* at this website:

`http://www.vmware.com/pdf/vsphere4/r41/vsp_41_iscsi_san_cfg.pdf`

### Datastore configuration for IP storage multipathing

In addition to properly configuring the virtual switches, network adapters, and IP addresses, use multiple physical paths simultaneously on an IP storage network.

Our examples show one or more VMkernel ports on multiple subnets, depending on whether you have stacked switches or nonstacked switches. The N series storage system has been configured with an IP address on each of the subnets used to access datastores. This was done to configure the interfaces of the VMware ESX Server, as shown in the previous examples. This configuration is accomplished by using multiple teamed adapters, each with their own IP address. Alternatively, in some network configurations, IP address aliases are assigned to the teamed adapters, allowing those adapters to communicate on all the required subnets.

When connecting a datastore to the server, the administrator chooses to configure the connection to use one of the IP addresses assigned to the N series storage system. When using NFS datastores, this configuration is accomplished by specifying the chosen IP address when mounting the datastore. When using iSCSI datastores, this configuration is accomplished by selecting the iSCSI LUN and specifying the preferred path.

Figure 4-10 shows an overview of storage traffic flow when using multiple VMware ESX Servers and multiple datastores with stacked switches.

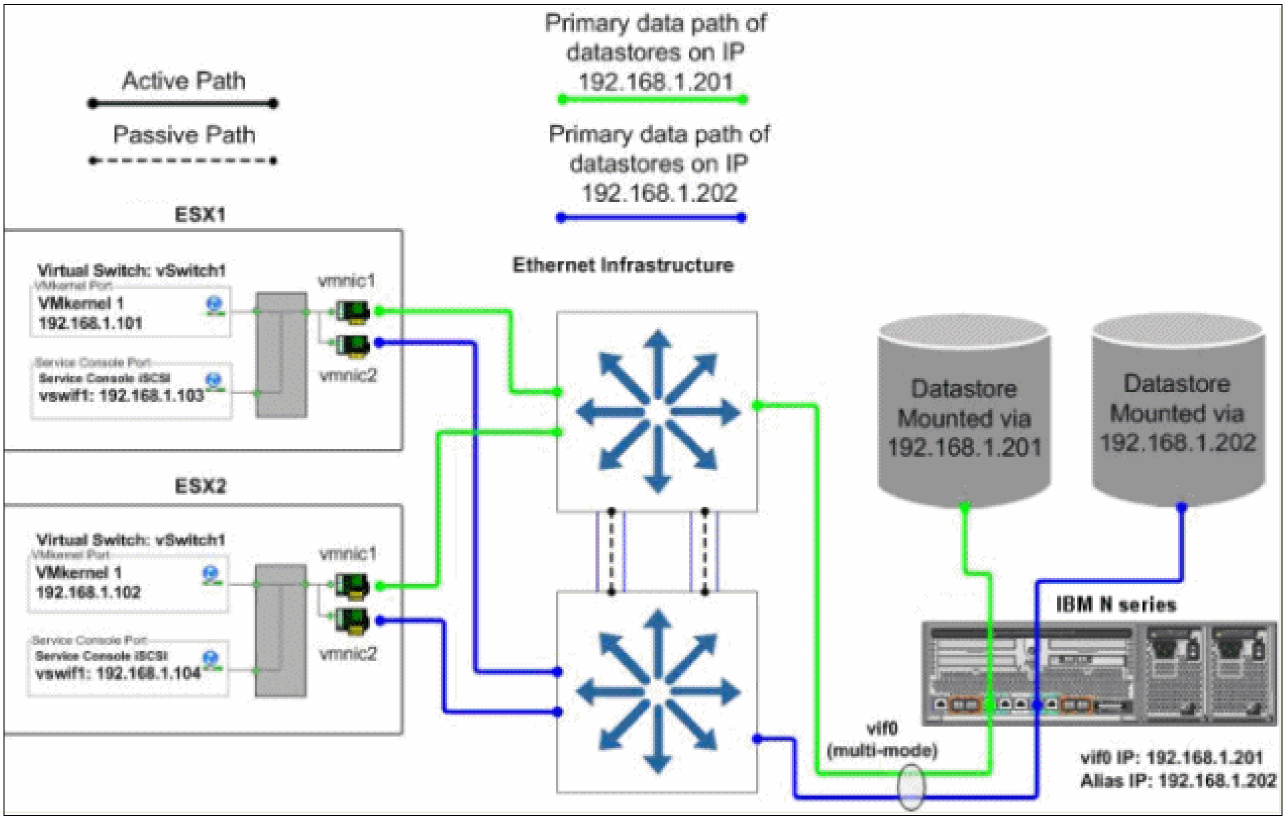



*Figure 4-10 Datastore connections with a stacked switch configuration*

Figure 4-11 shows an overview of storage traffic flow when using multiple VMware ESXi Servers and multiple datastores with nonstacked switches.

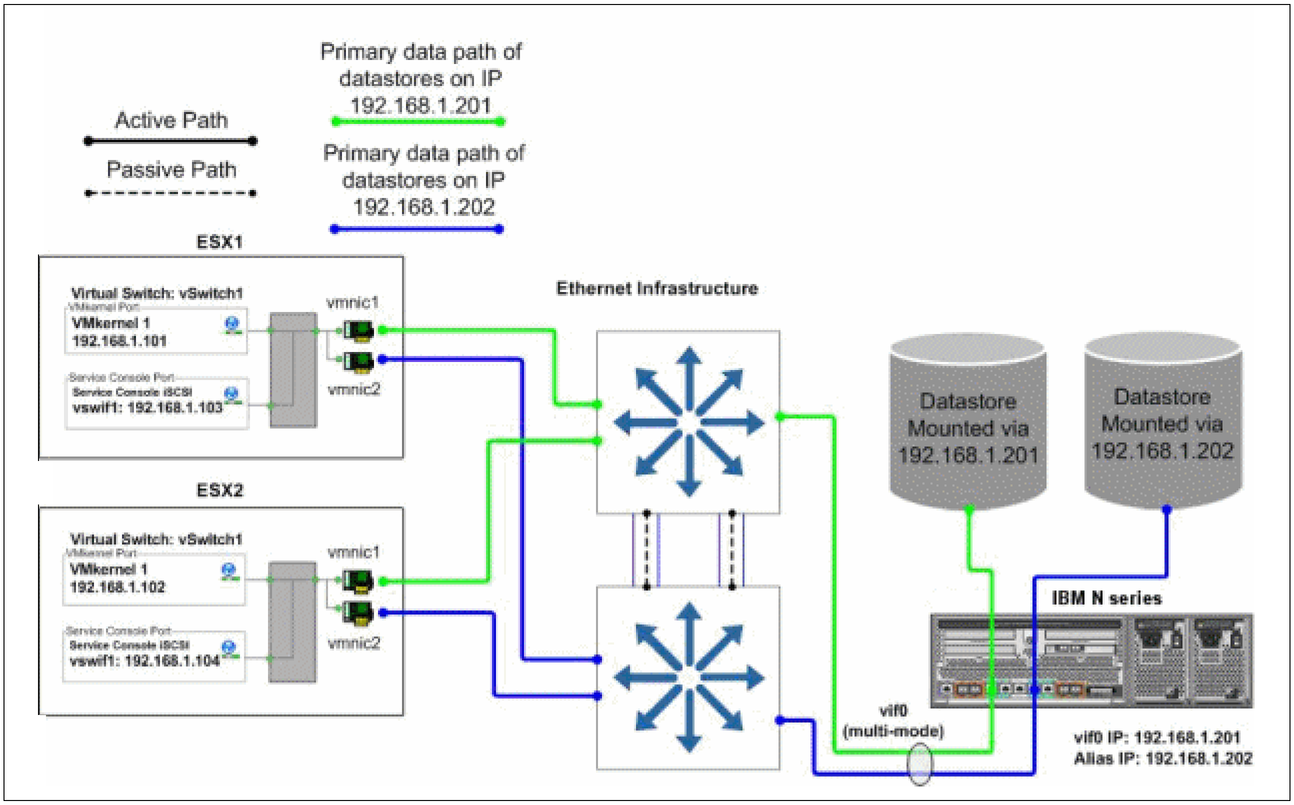



*Figure 4-11 Datastore connections with a non-stacked switch configuration*

## VMware ESXi Server adapter failover behavior

VMware ESXi Server adapter failure (caused by a cable pull or NIC failure) is where traffic originally running over the failed adapter is rerouted. It continues through the second adapter, but on the same subnet where it originated. Both subnets are now active on the surviving physical adapter. Traffic returns to the original adapter when service to the adapter is restored.

## Switch failure

Traffic originally running to the failed switch is rerouted and continues through the other available adapter, through the surviving switch, to the N series storage system. Traffic returns to the original adapter when the failed switch is repaired or replaced.

Figure 4-12 shows the data flow during normal operation.

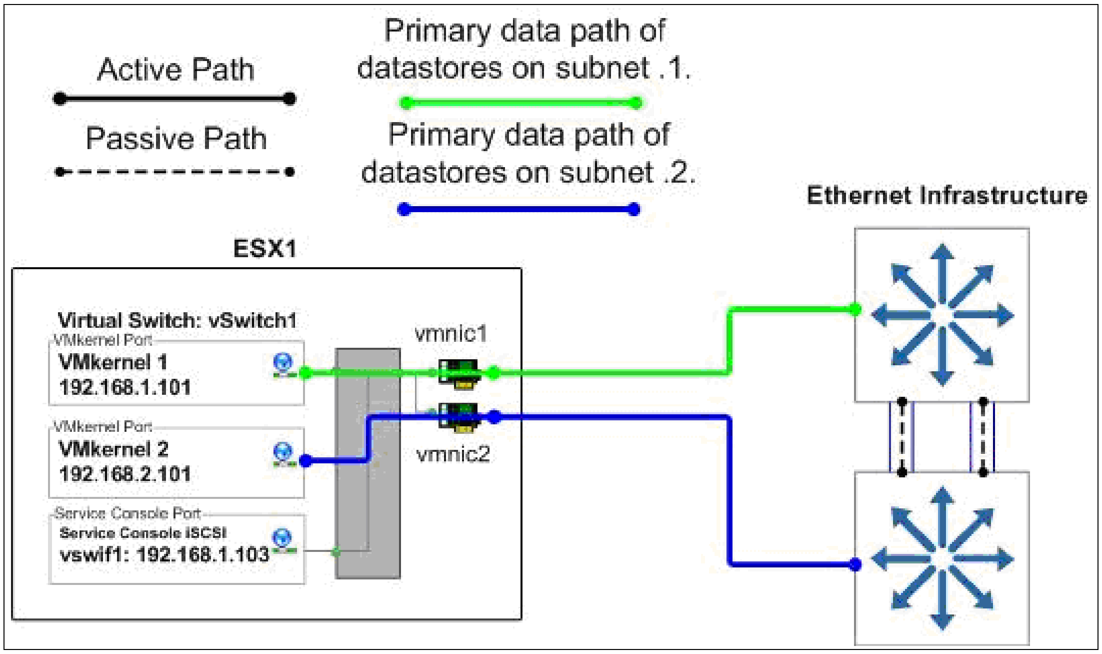



*Figure 4-12 VMware ESX Server Switch1 normal operation*

Figure 4-13 shows the data flow when a switch is unavailable.

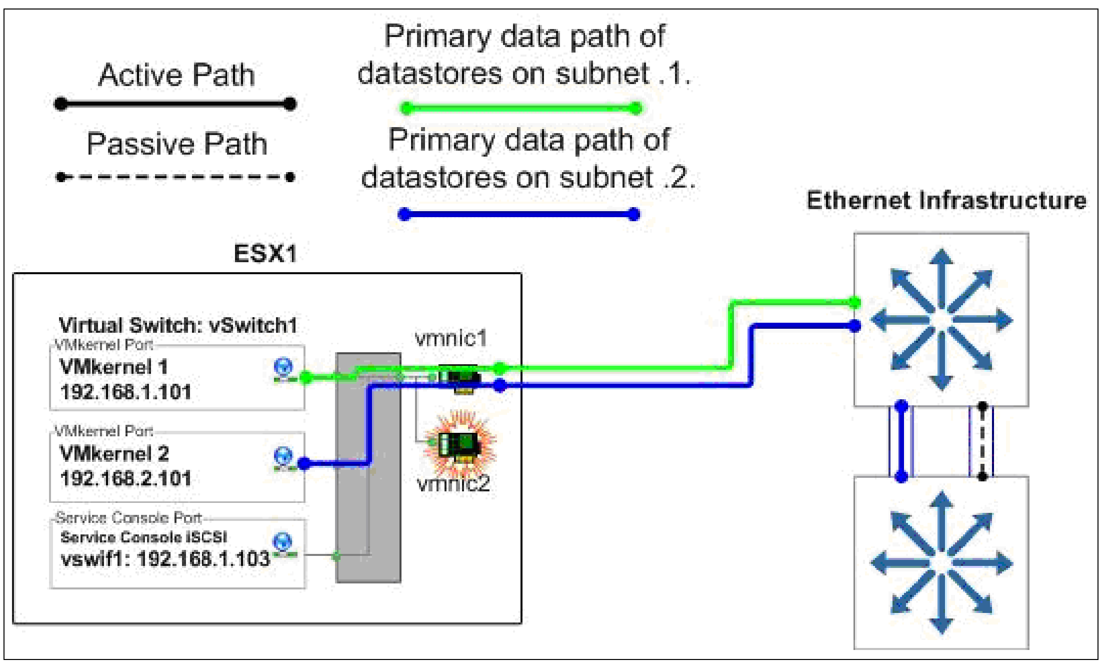



*Figure 4-13 VMware ESX Server Switch1 unavailable operation*

## 4.6.3 Network configuration options for the N series storage system

This section examines the networking options from the N series perspective.

### Option 1: Storage-side multimode VIFs with LACP

If the switches to be used for IP storage networking support cross-stack EtherChannel trunking, each storage controller only needs one physical connection to each switch. The two ports connected to each storage controller are then combined into one multimode Link Aggregation Control Protocol (LACP) VIF, with IP load balancing enabled. Multiple IP addresses can be assigned to the storage controller using IP address aliases on the VIF.

This option has the following advantages:

- It provides two active connections to each storage controller.
- It easily scales to more connections.
- Storage controller connection load balancing is automatically managed by EtherChannel IP load balancing policy.

This option has the disadvantage that not all switch vendors or switch models support cross-switch EtherChannel trunks.

Figure 4-14 shows how option 1 is configured.

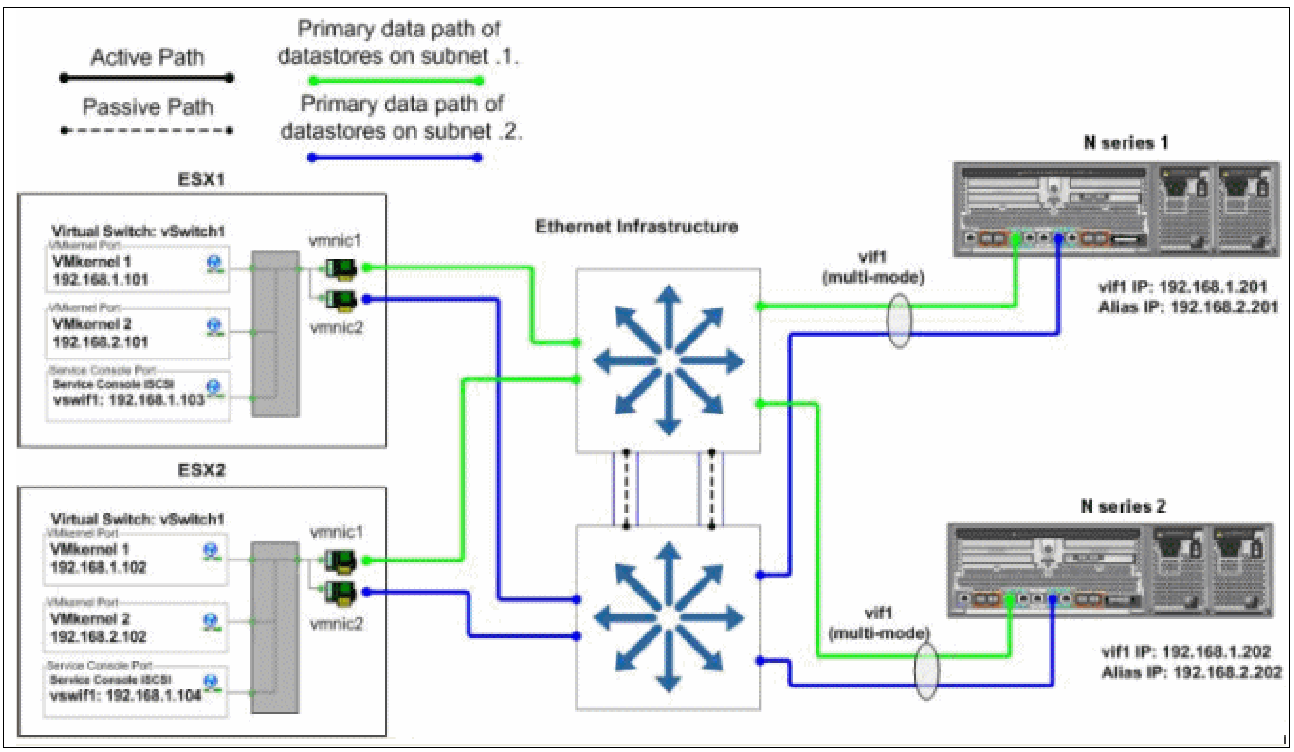



*Figure 4-14 Storage-side multimode VIFs using LACP across stacked switches*

### Option 2: Storage-side single mode VIFs

In this configuration, the IP switches to be used do not support cross-stack trunking. Therefore, each storage controller requires four physical network connections. The connection is divided into two single mode (active/passive) VIFs. Each VIF has a connection to both switches and a single IP address assigned to it. The **`vif favor`** command is used to force each VIF to use the appropriate switch for its active interface.

This option has the following advantages:

- No switch-side configuration is required.
- It provides two active connections to each storage controller.
- It scales for more connections.

This option has the disadvantage that it requires two physical connections for each active network connection. Figure 4-15 shows how option 2 is configured.

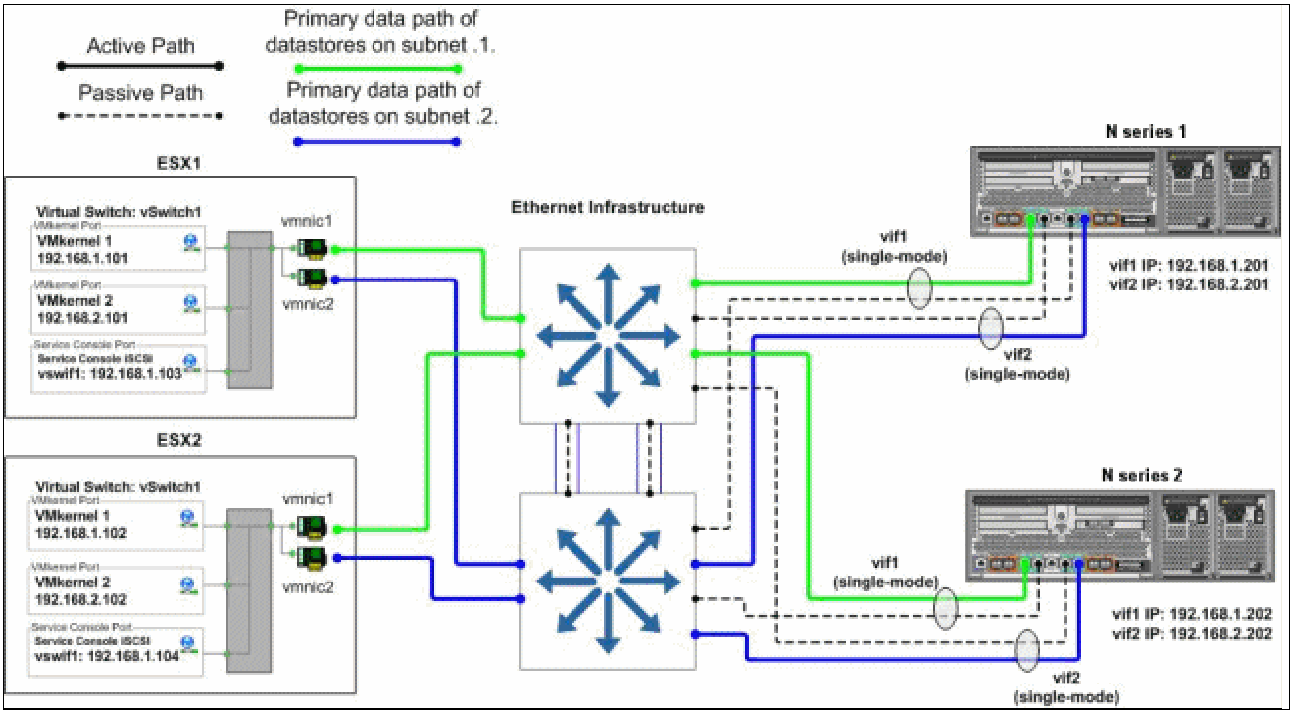



*Figure 4-15 Storage-side single mode VIFs*

## Option 3: Storage-side multimode VIFs

In this configuration, the IP switches to be used do not support cross-stack trunking. Therefore, each storage controller requires four physical network connections. The connections are divided into two multimode (active/active) VIFs with IP load balancing enabled, with one VIF connected to each of the two switches. These two VIFs are then combined into one single mode (active/passive) VIF. Multiple IP addresses can be assigned to the storage controller using IP address aliases on the single mode VIF.

This option has the following advantages:

- It provides two active connections to each storage controller.
- It scales for more connections.
- Storage controller connection load balancing is automatically managed by EtherChannel IP load balancing policy.

This option has the following disadvantages:

- It requires two physical connections for each active network connection.
- Some switch-side configuration is required.
- Some storage traffic can cross the uplink between the two switches.

Figure 4-16 shows how option 3 is configured.

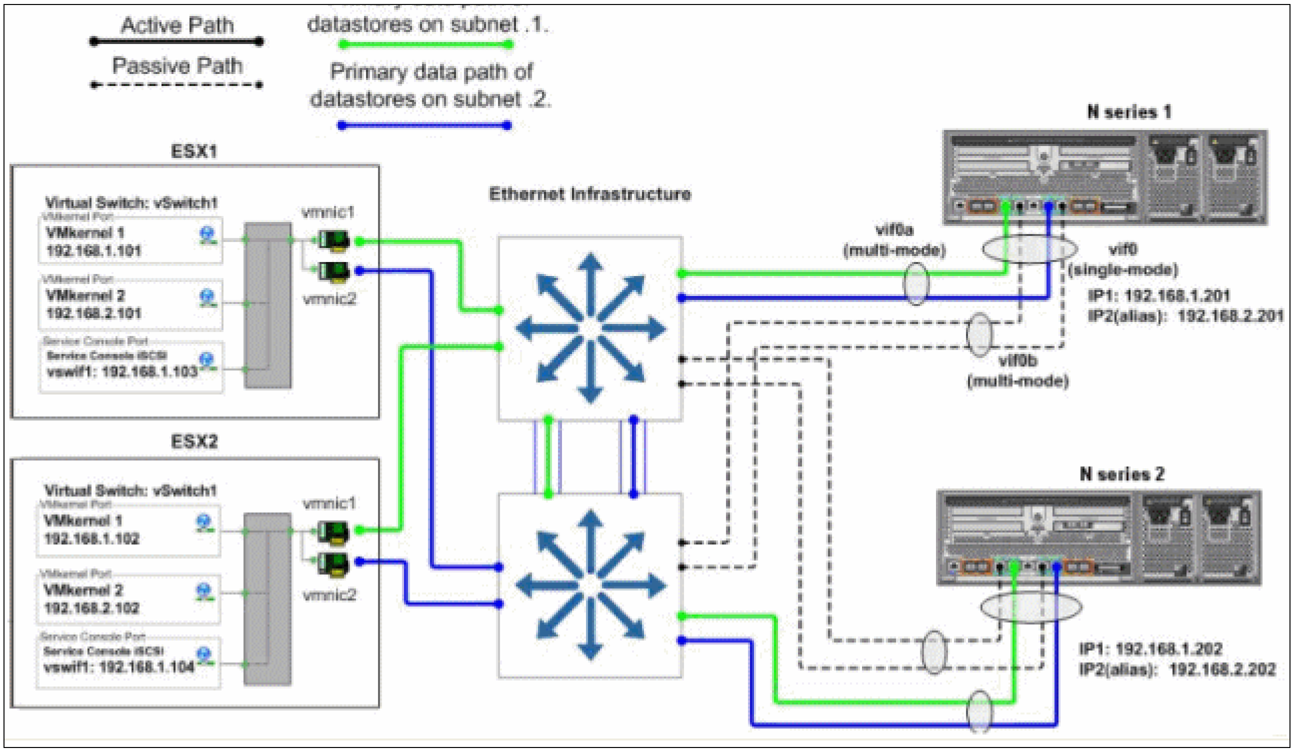



*Figure 4-16 Storage-side multimode VIFs*

### Failover behavior of an N series network connection

This section explores the failure behavior of an N series network connection.

#### *Storage controller connection failure (link failure)*

Depending on the N series configuration option used, traffic from the VMware ESX Server is routed through the other switch or to one of the other active connections of the multimode VIF. Traffic returns to the original connection when service to the connection is restored.

#### *Switch failure*

Traffic originally running to the failed switch is rerouted and continues through the other available adapter, through the surviving switch, to the N series storage system. Traffic returns to the original adapter when the failed switch is repaired or replaced.

#### *Storage controller failure*

The surviving controller services requests to the failed controller after a cluster takeover. All interfaces on the failed controller are automatically started on the surviving controller. Traffic returns to the original controller when it returns to normal operation.

## 4.7 Increasing storage utilization

VMware provides a means of increasing the hardware utilization of physical servers. By increasing hardware utilization, the amount of hardware in a data center can be reduced, thus lowering the cost of data center operations. In a typical environments, the process of migrating physical servers to virtual machines does not reduce the amount of data stored or the amount of storage provisioned. By default, server virtualization does not have any impact on improving storage utilization, and in many cases might have the opposite effect.

By using deduplication and storage thin provisioning, higher density of storage utilization can be achieved.

Another element to consider is the configuration of transient volumes.

## 4.7.1 N series deduplication

By providing deduplication options, the N series can provide important benefits to vSphere environments.

### Deduplication considerations with VMFS and RDM LUNs

Enabling deduplication when provisioning LUNs produces storage savings. However, the default behavior of a LUN is to reserve an amount of storage equal to the provisioned LUN. This design means that although the storage array reduces the amount of capacity consumed, any gains made with deduplication are usually unrecognizable. This occurs because the space reserved for LUNs is not reduced.

To recognize the storage savings of deduplication with LUNs, you must enable LUN thin provisioning. In addition, although deduplication reduces the amount of consumed storage, this benefit is not seen directly by the VMware ESX Server administrative team. Their view of the storage is at a LUN layer, and as explained earlier, LUNs always represent their provisioned capacity, whether they are traditional or thin provisioned.

### Deduplication considerations with NFS

Unlike with LUNs, when deduplication is enabled with NFS, the storage savings are both immediately available and recognized by the VMware ESX Server administrative team. No special considerations are required for its usage.

## 4.7.2 Storage thin provisioning

You are probably familiar with traditional storage provisioning and the way in which storage is pre-allocated and assigned to VMs. A common practice for server administrators is to over provision storage to avoid running out of storage and the associated application downtime when expanding the provisioned storage. Although no system can be run at 100% storage utilization, storage virtualization methods allow administrators to address and over subscribe storage in the same manner as with server resources, such as CPU, memory, networking, and so on. This form of storage virtualization is referred to as *thin provisioning*.

### Thin provisioning principles

Thin provisioning provides storage on demand, where traditional provisioning pre-allocates storage. The value of thin-provisioned storage is that storage is treated as a shared resource pool and is consumed only as each individual guest requires it. This sharing increases the total utilization rate of storage by eliminating the unused but provisioned areas of storage that are associated with traditional storage. The drawback to thin provisioning and over subscribing storage is that, without the addition of physical storage, if every guest requires its maximum storage at the same time, there is not enough storage to satisfy the requests.

### N series thin provisioning options

N series thin provisioning allows LUNs that are serving VMFS datastores to be provisioned to their total capacity limit yet consume only as much storage as is required to store the VMDK files (of either thick or thin format). In addition, LUNs connected as RDMs can be thin provisioned.

### 4.7.3 Elements of thin provisioning

Thin provisioning can be performed at the volume level and the LUN level. To see the space savings when using N series deduplication on LUNs being presented to VMware hosts, you must enable LUN-level thin provisioning. The space savings using the Network File System (NFS) are immediately available.

#### Volume-level thin provisioning

Volumes can be set to a space guarantee of Volume, File, or None. By default, volumes are created with a space guarantee of *Volume*, which pre-allocates the size of the volume within the aggregate. No other application can use it, even if it is empty space.

When you enable the space guarantee to *None*, you enable volume-level thin provisioning. With volume-level thin provisioning, you can create volumes larger than the size of the aggregate. Also, the space gets allocated when the application writes to it.

A space guarantee of *File* pre-allocates space in the volume. In this case, any file in the volume with space reservation enabled can be rewritten, even if its blocks are marked for a Snapshot.

#### LUN-level thin provisioning

During the creation of a LUN, you can select **Space Reserved**. Alternatively, you can clear the option and enable thin provisioning on the LUN. If you select **Space Reserved**, the total space of the LUN is pre-allocated in the volume. Even though the space is not being used by the LUN, it is not accessible for use by any other LUN in the volume.

If you clear the **Space Reserved** option, the unused space in the volume can be claimed by another volume, thus maximizing storage usage.

## 4.8 Snapshots

This topic provides information about the backup and recovery techniques and technologies that you can use with a VMware vSphere 4.1 and N series solution.

VMware is capable of taking a Snapshot of guests, which enables you to make point-in-time copies that provide the fastest means to recover a guest to a previous point in time. N series storage systems have been providing customers with the ability to create Snapshot copies of their data since its introduction. The basic concept of a Snapshot is similar between N series systems and VMware. However, be aware of the major differences between the two technologies and when to use one rather than the other.

VMware snapshots provide simple point-in-time versions of guests, allowing quick recovery. The benefits of VMware snapshots are the easy way to create and use them, because they can be executed and scheduled from within vCenter.

> **Tip:** Do not use the Snapshot technology in VMware as the only way to back up your virtual infrastructure.

For more information about native VMware snapshots, including usage guidelines, see the *Datacenter Administration Guide* at the following website:

http://www.vmware.com/pdf/vsphere4/r41/vsp_41_dc_admin_guide.pdf

The patented N series Snapshot technology can easily be integrated into VMware environments. This technology provides crash-consistent versions of guests for full guest recovery, full guest cloning, or site replication and disaster recovery. The benefits of this solution are that it is the storage industry's only Snapshot technology that does not have a negative impact on system performance. VMware states that, for optimum performance and scalability, hardware-based Snapshot technology is preferred over software-based solutions. The limitation of this solution is that it is not managed within VMware vCenter, requiring external scripting or scheduling to manage the process.

## 4.9 N series FlexShare

VMware vSphere 4.1 provides options for memory reservations. These techniques provide administrators the ability to ensure that certain guests, or a group of guests, get the memory needed to achieve the performance required. In a similar fashion, IBM System Storage N series systems provide a workload prioritization method called *FlexShare*.

FlexShare prioritizes processing resources for key services when the system is under heavy load. FlexShare does not provide guarantees on the availability of resources or how long particular operations take to complete. FlexShare provides a priority mechanism to give preferential treatment to higher priority tasks.

With the use of FlexShare, administrators can confidently consolidate different applications and data sets on a single storage system. FlexShare gives administrators the control to prioritize applications based on how critical they are to the business (Figure 4-17).

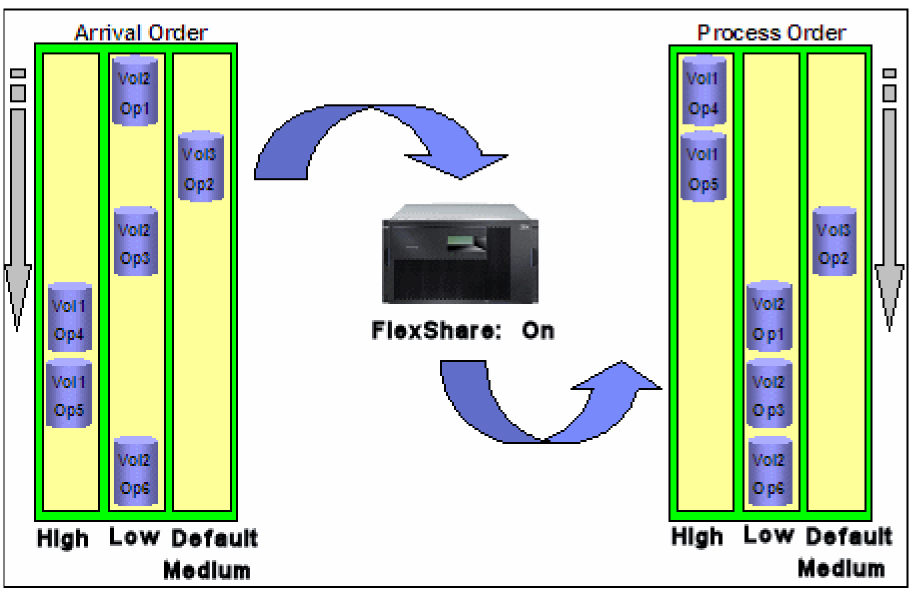



*Figure 4-17 FlexShare prioritization*

FlexShare is supported on N series storage systems running Data ONTAP Version 7.2 and later.

FlexShare provides storage systems with the following key features:

- Relative priority of different volumes
- Per-volume user versus system priority
- Per-volume cache policies

By using these features, storage administrators can set how the system must prioritize resources when the storage is overloaded.

**Priority settings:**

- Before configuring priority on a storage system, you must understand the different workloads on the storage and the impact of setting priorities. Improperly configured priority settings can have undesired effects on application and system performance. The administrator must be well-versed in the configuration implications and best practices.
- For additional information about FlexShare, see *IBM System Storage N series with FlexShare*, REDP-4291.

# 4.10 Licensing

You can employ numerous advanced features for your virtual data center. Many of these features require you to purchase nothing more than an additional license to activate the feature. This topic addresses the types of licensing.

## 4.10.1 VMware licensing

VMware provides a free hypervisor, which is the software to enable the "hardware partitioning" to create virtual machines. It is basically an ESXi, which alone does not provide redundancy and resiliency features as vMotion. You can download it at this website:

http://www.vmware.com/products/vsphere-hypervisor/overview.html

With the purchase of VMware vCenter, you can enable the following features with the addition of a license key and an additional server, when required:

- VCenter Agent for ESX Server
- VMotion
- VMware High Availability
- VMware Dynamic Resource Scheduling
- VMware Consolidated Backup
- VMware Fault Tolerance.

For additional information about VMware vSphere components and requirements, see this website:

http://www.vmware.com/products/vsphere/overview.html

### 4.10.2 N series licensing

With the purchase of an IBM System Storage N series system, you can enable features with the addition of a license key. The software licensing structure has been changed with the introduction on the N62xx models. An overview of different licensing options is provided in Figure 4-18.

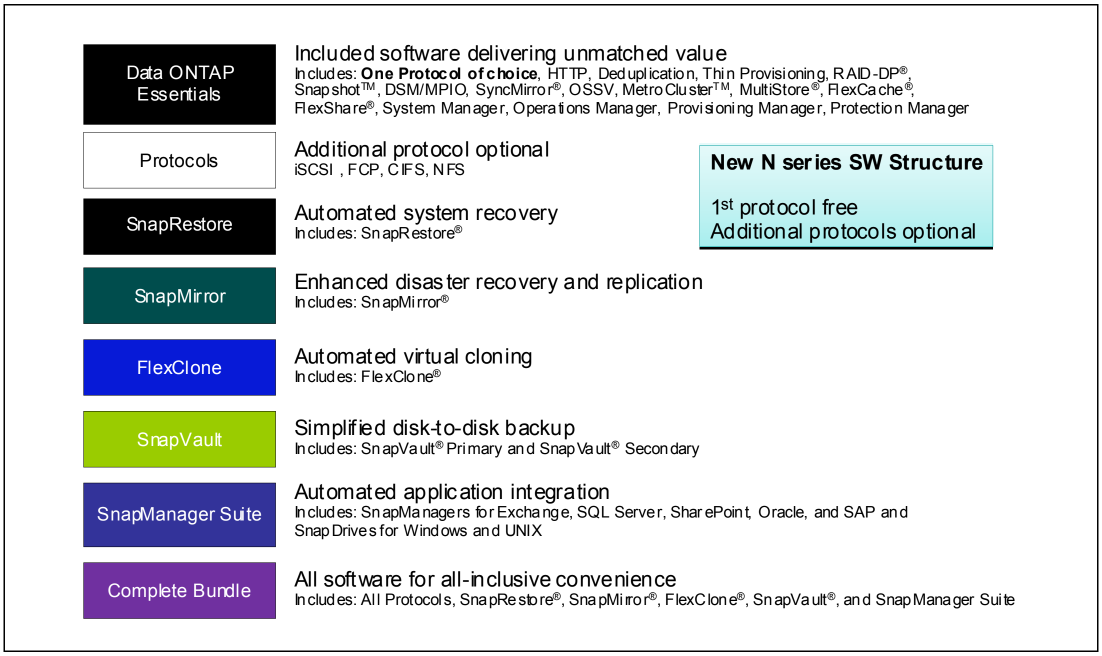



*Figure 4-18 N series software structure*

Again, you must ensure that any necessary features for your environment are licensed.

For additional information about N series advanced features and their requirements, see the NAS page at this website:

http://www-03.ibm.com/systems/storage/network/index.html

# 5

# Installing the VMware ESXi 4.1 using N series storage

This chapter explains how to install and configure the VMware ESXi 4.1 operating system by using local disks on a server. It includes the following topics:

- Pre-installation tasks
- Installing the ESXi operating system

## 5.1 Pre-installation tasks

Before having your VMWare host running, serving your virtual machines with hardware resources, it is a good idea to check the integrity of them. A good practice is to run memory tests for 48 hours before installing VMWare ESXi to ensure that the hardware is OK to enter into production.

We are installing ESX 4.1 Update 1 in a local disk, so the installation is straightforward. We just need to check whether the server is able to find the local disk using the local storage adapter. Then we create a logical volume as a RAID 1, also known as a mirrored drive.

If you are using the boot-from-SAN feature of VMware ESX, before starting the installation of the operating system, you need to perform the following tasks:

- Ensure that the logical unit number (LUN) is properly created and mapped in the N series.
- Ensure that the fiber connection between the N series system and the server is done through a SAN switch.
- Verify that the LUN zoning is properly set up in the SAN switch.
- Ensure that the server's HBA is configured to be bootable.
- Set up the correct boot sequence by using the Basic Input/Output System (BIOS) of the server.

> **Preferred practice:** If for any reason the server already has data LUNs zoned, unzone them before installing the operating system to avoid data loss. Leave only the LUN for the ESXi installation zoned to the server.

- Download ESXi 4.1 OS installation ISO from the VMware website:

  `http://www.vmware.com/download/download.do?downloadGroup=ESXI41U1`

## 5.2 Boot options for VMware ESXi Servers

You can choose to install the VMware ESXi Server on your local drive or in a storage LUN, also known as boot from storage area network (SAN). To help you to decide what option to use, consider the most beneficial setup for your environment. Here are some guidelines to help you decide what to use:

- Install the VMware ESXi by using local drives:

  Choose this option if you have the following situations:

  - You have storage space problems.
  - You are concerned with troubleshooting if you lose SAN connectivity.

- Install the VMware ESXi by using boot from a SAN:

  Choose this option if you have the following situations:

  - You are concerned about local hard disk maintenance and an extra level of redundancy.
  - You are installing ESXi in a diskless blade system.
  - You want to be able to clone the ESXi operating system for multiple future deploys or for disaster recovery purposes.

**Boot from SAN:** VMWare supports boot from SAN by using Fibre Channel Protocol (FCP) or the iSCSI protocol. When using iSCSI, it is only supported if it is hardware initiated.

## 5.3 Preparing N series for the VMware ESXi Server

To boot from SAN and install the ESXi operating system in the server, prepare the storage system to accommodate the boot LUN. Complete the items on the following checklist before you begin:

1. Check the hardware elements, such as host bus adapters (HBAs), and storage devices. They must be compatible and configured according to the boot from SAN requirements. Note the following requirements:

   - HBA. The BIOS of the HBA Fibre Channel must be enabled and configured for boot from SAN. See the HBA setup in 5.3.3, “Configuring Fibre Channel HBA for boot from SAN” on page 82.
   - LUN. The bootable LUN cannot be shared between other servers. Only the ESXi Server that is actually using the LUN can use the LUN.

2. When you boot from an active/passive storage array, the Storage Processor whose worldwide port name (WWPN) is specified in the BIOS configuration of the HBA must be active. If that Storage Processor is passive, the HBA cannot support the boot process.
3. Make the fiber connection between the N series and the server through a SAN switch. Boot from SAN is not supported if the storage and the server are directly connected. The boot LUN must be properly zoned in the SAN switch.

## 5.3.1 Preparing N series LUNs for the ESXi boot from SAN

To set up a LUN in the N series to be used as a bootable LUN for the ESXi server:

1. Log in to the N series FilerView (GUI interface):

   a. Launch an Internet browser and type in the following URL:

   `http://<nseries_address>/na_admin`

   Where *nseries_address* is the host name or IP address of your N series storage system.

   b. Enter a user name and password, as shown in Figure 5-1.

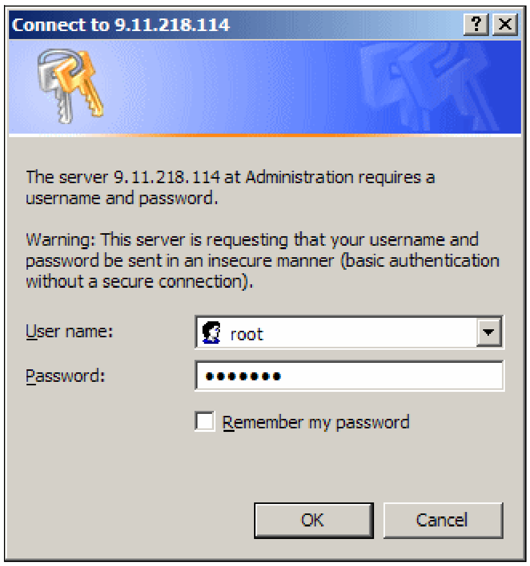



*Figure 5-1 N series Overview authentication window*

   c. When you are authenticated, in the Data ONTAP main window (Figure 5-2), click the **FilerView** icon to go to the control page.

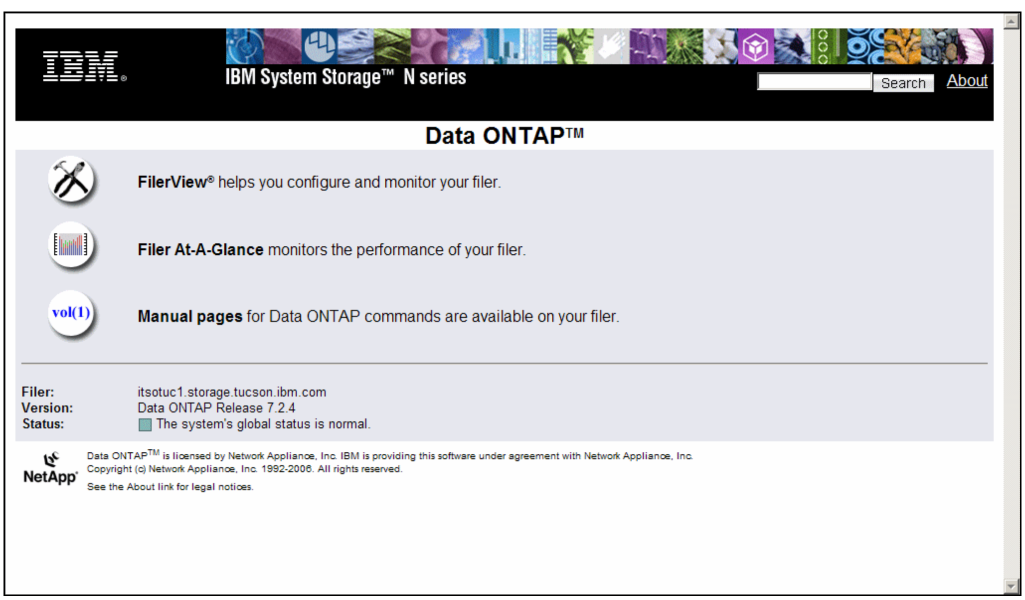



*Figure 5-2 FilerView main window*

The main menu bar in the left pane of the window is displayed. From there, you can control most of the features of the storage system, as shown in Figure 5-3.

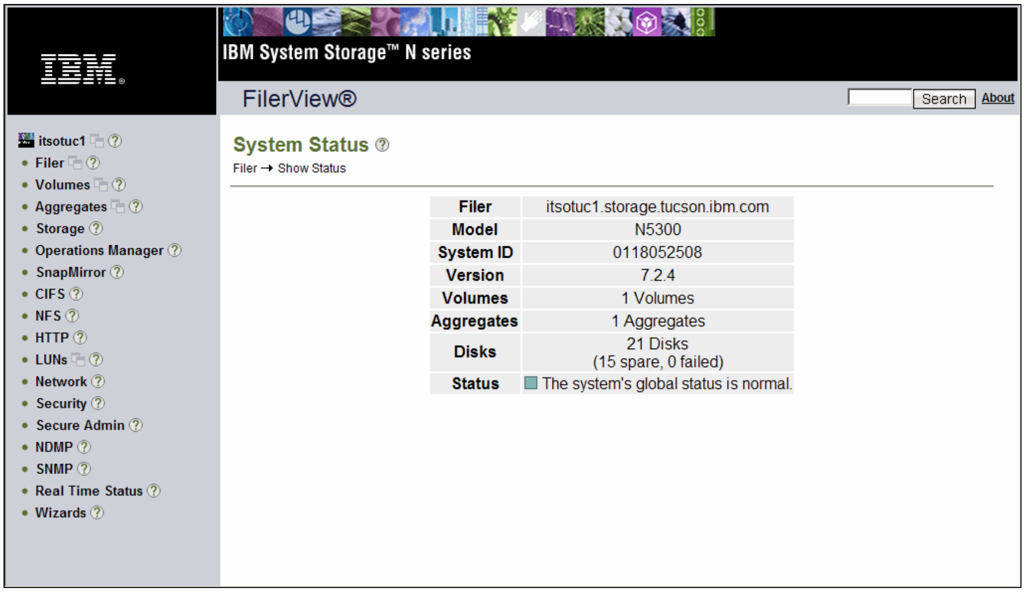



*Figure 5-3 Main menu window*

2. Create an aggregate:

   a. In the left pane of the FilerView panel, select **Aggregates** → **Add** (Figure 5-4).

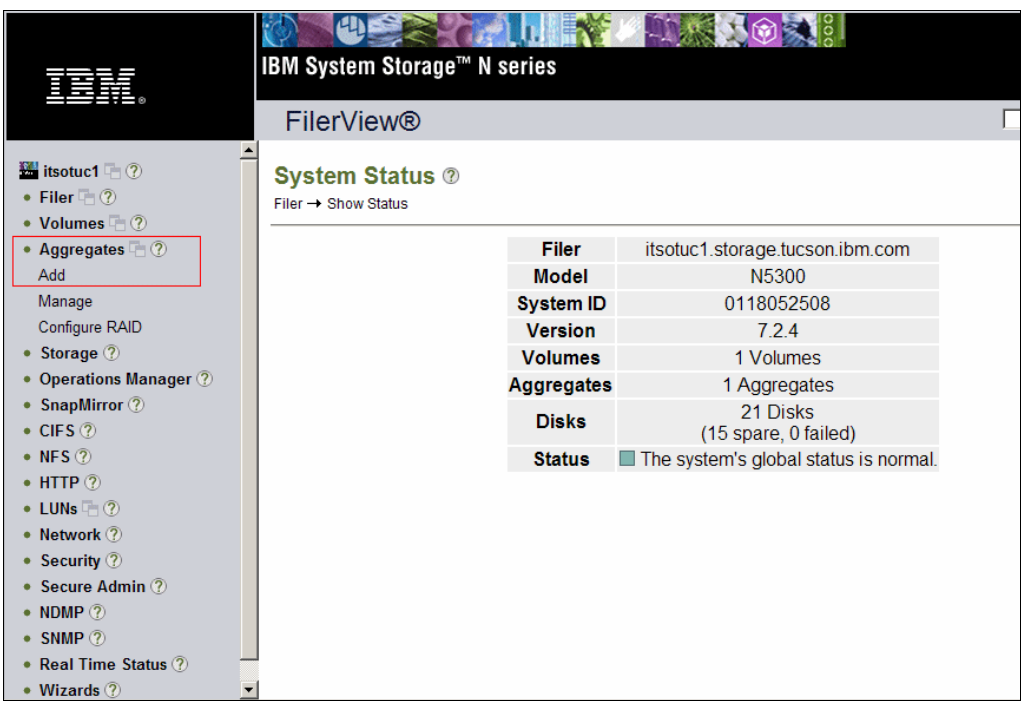



*Figure 5-4 Selecting the option to add an aggregate*

b. In the Aggregate Wizard window (Figure 5-5), click **Next**.

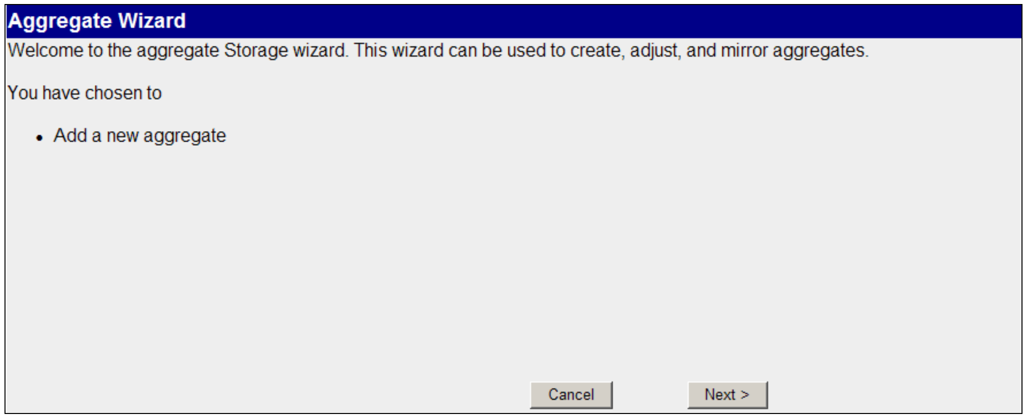



*Figure 5-5 Aggregate Wizard Welcome window*

c. In the Aggregate Parameters panel (Figure 5-6), give the aggregate a name. In this example, we call it `esx_boot`. Select the **Double Parity** check box if you want to use RAID-DP level. Click **Next**.

**RAID-DP:** With RAID-DP, you can continue serving data and recreate lost data even if you have two failed disks.

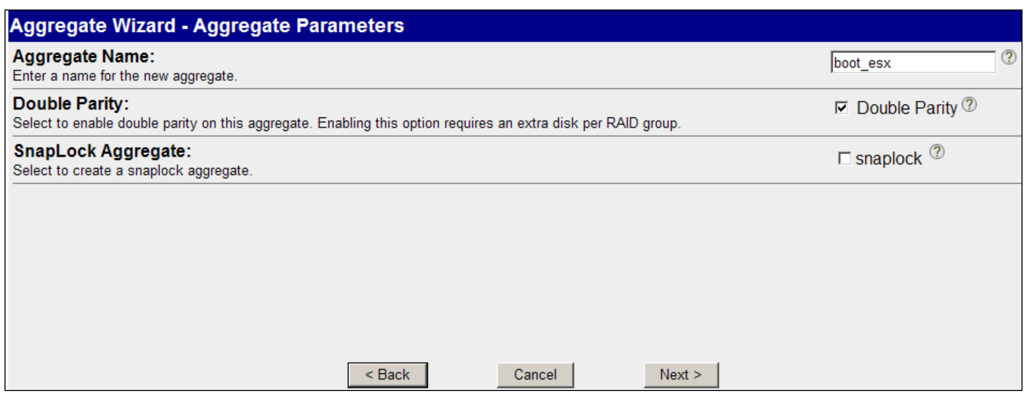



*Figure 5-6 Naming the aggregate*

d. In the RAID Parameters panel (Figure 5-7), from the drop-down list, select the number of physical disks per RAID that are to be part of this aggregate. Click **Next**.

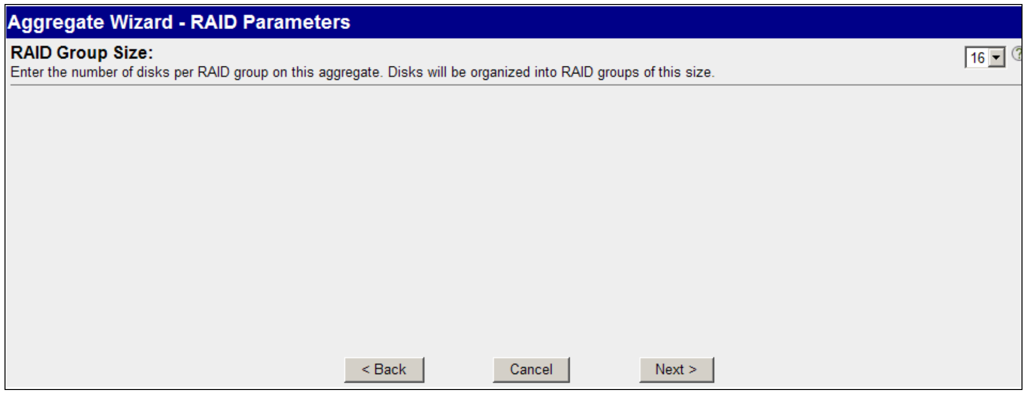



*Figure 5-7 Specifying the number of disks per RAID*

e. In the Disk Selection Method panel (Figure 5-8), select whether you want disk selection to be performed automatically or manually. In this example, we select **Automatic** so that the storage system can decide which physical drives to use. However, if you are in a mixed drive environment, you can select **Manual**. Click **Next**.

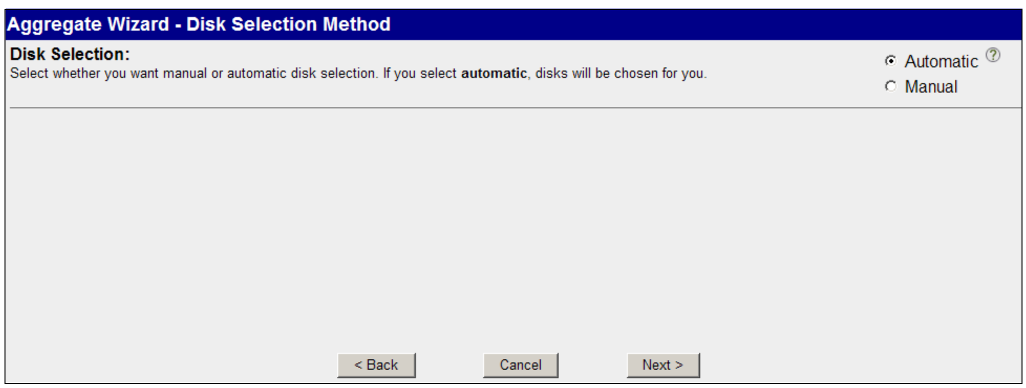



*Figure 5-8 Selecting the type of disk selection (automatic in this example)*

f. In the Disk Size panel (Figure 5-9), select the disk size that is to be part of the aggregate. If you have more than one unique disk size in your storage system, you can force the use of disks of a specific size, or leave the default of Any Size. In this case, we select **Any Size**. Click **Next**.

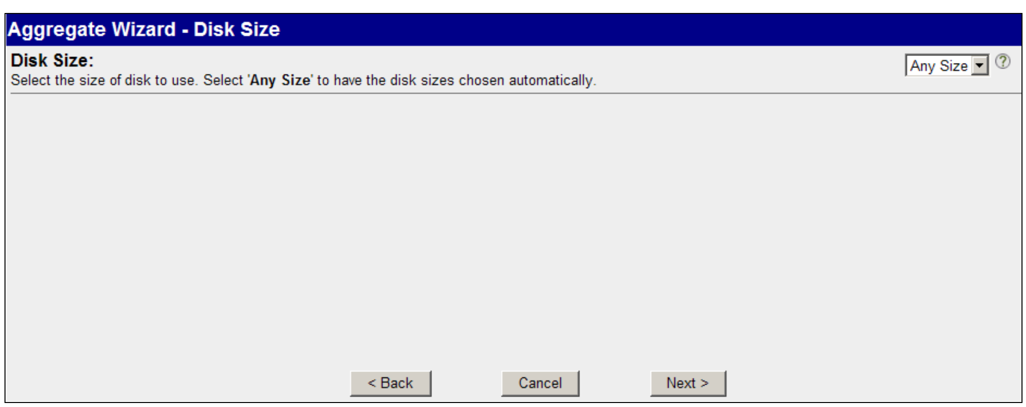



*Figure 5-9 Aggregate setup - disk size selection*

g. After the disk size is determined, in the Number of Disks panel (Figure 5-10), use the drop-down list. Select the number of disks to use in this aggregate, depending on the size of the aggregate you want. Click **Next**.

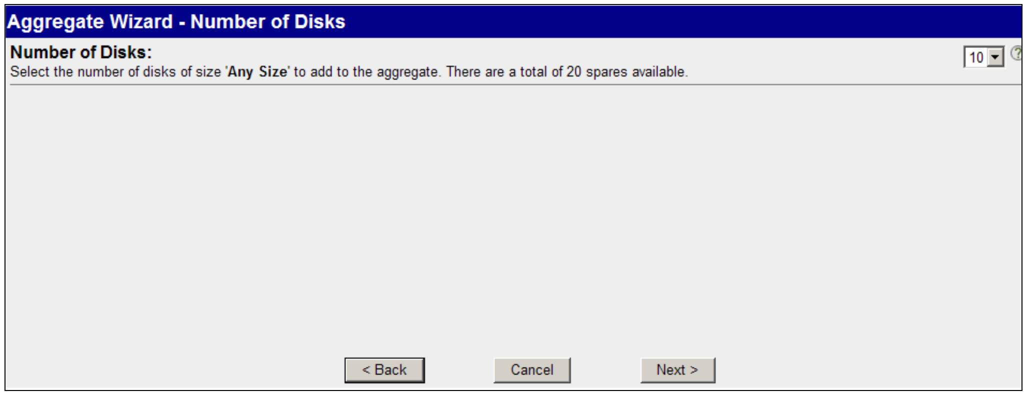



*Figure 5-10 Selecting the number of disks to use in the aggregate*

h. In the Commit panel (Figure 5-11), which summarizes the settings, click **Commit**.

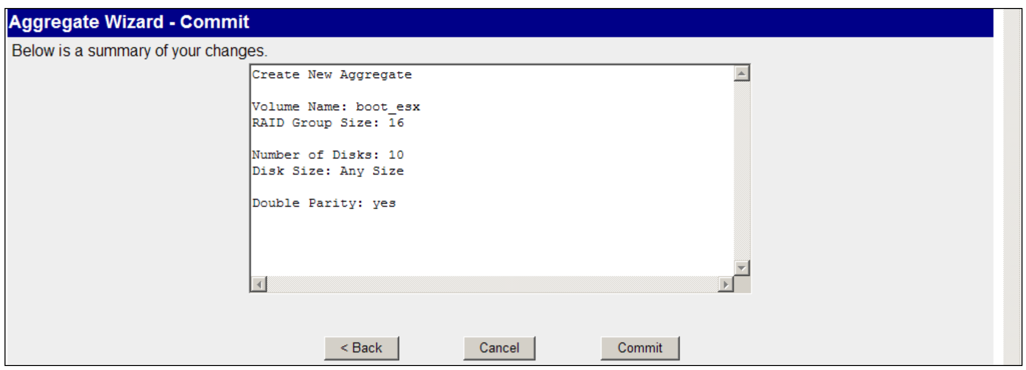



*Figure 5-11 Committing the aggregate setup*

i. After the aggregate is created, in the left pane of the FilerView window (Figure 5-12), find the aggregate by selecting **Aggregate** → **Manage**.

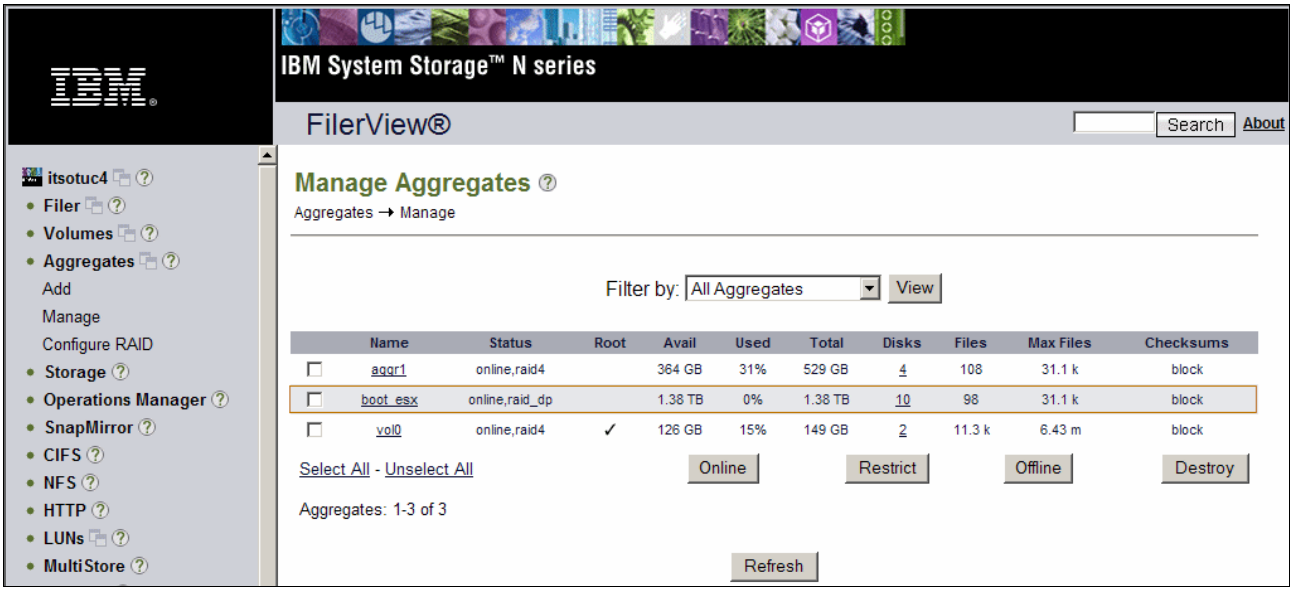



*Figure 5-12 New aggregate*

3. After the aggregate is defined, create a volume:

   a. In the left pane of the FilerView panel, select **Volume** → **Add**.

   b. In the Volume Wizard panel (Figure 5-13), click **Next**.

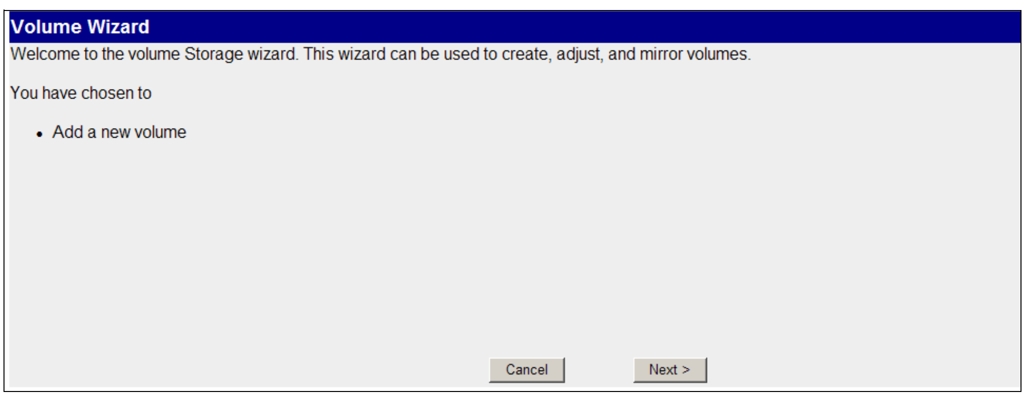



*Figure 5-13 Volume Wizard Welcome panel*

c. In the Volume Type Selection panel (Figure 5-14), select **Flexible** or **Traditional** depending on the type of volume to be created:

- With Flexible volumes, you can shrink or grow the volume size at a later time without service interruption or data loss.
- By choosing Traditional volumes, you cannot resize the volume.

In this example, we choose the **Flexible** option. Click **Next**.

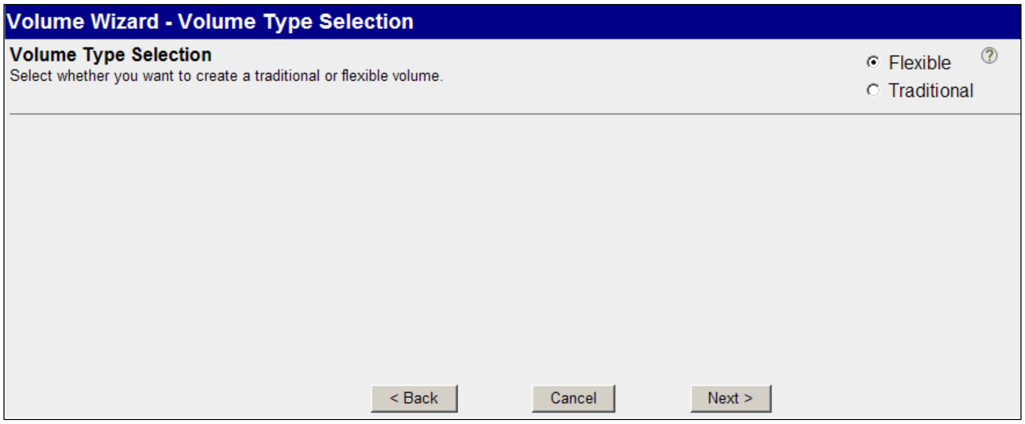



*Figure 5-14 Setting the volume type*

d. In the Volume Parameters panel (Figure 5-15), give the new volume a name. In this example, the volume name is boot_esx1. Click **Next**.

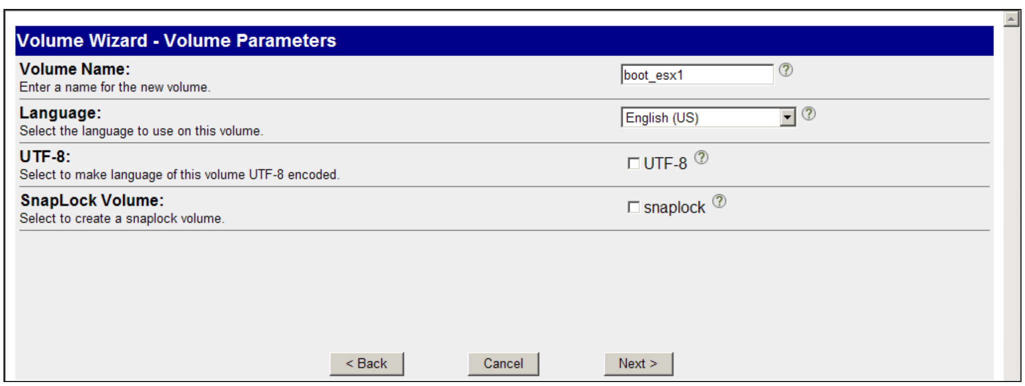



*Figure 5-15 Defining the volume parameters*

e. The volume is mounted over an aggregate structure. In the Flexible Volume Parameters panel (Figure 5-16), select the aggregate that you created in step 2 on page 65 to link the new volume. Click **Next**.

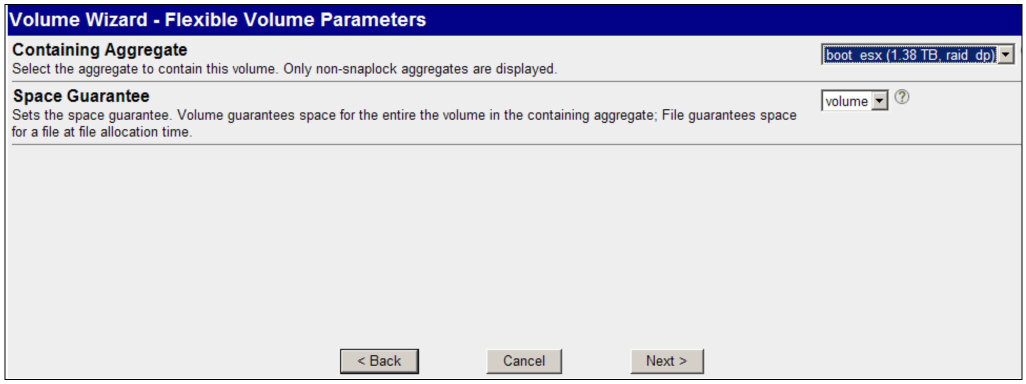



*Figure 5-16 Linking the aggregate to the new volume*

f. In the Flexible Volume Size panel (Figure 5-17), choose the volume size and the amount of space reserved to Snapshot. If you do not want to reserve space for snapshots, type 0 in the corresponding field. In this example, we create a 20 GB volume, reserving 10% of this size for snapshots.

Click **Next**.

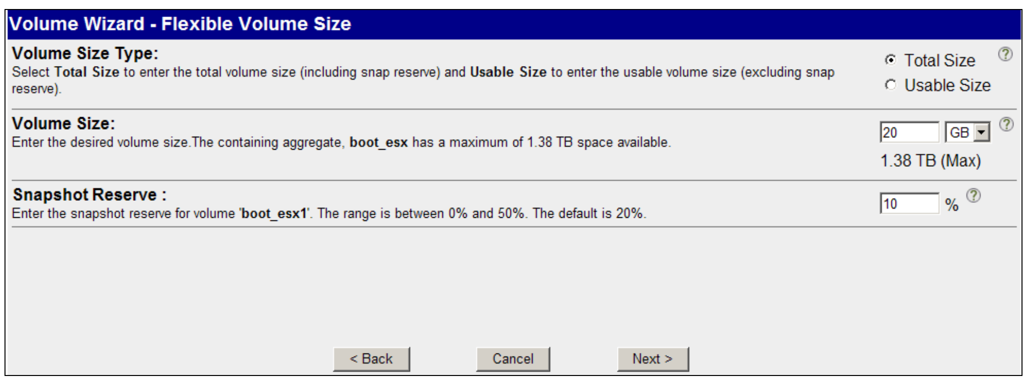



*Figure 5-17 Specifying the volume size and space for Snapshot*

g. In the Commit panel (Figure 5-18), which summarizes the settings, click **Commit**.

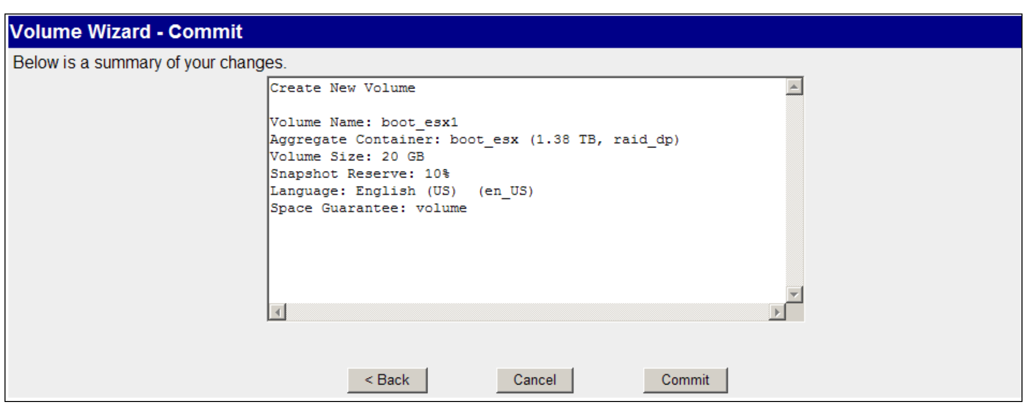



*Figure 5-18 Committing the settings for the volume*

h. After the volume is created, in the left pane of the FilerView panel (Figure 5-19), select **Volumes** → **Manage** to view the volume.

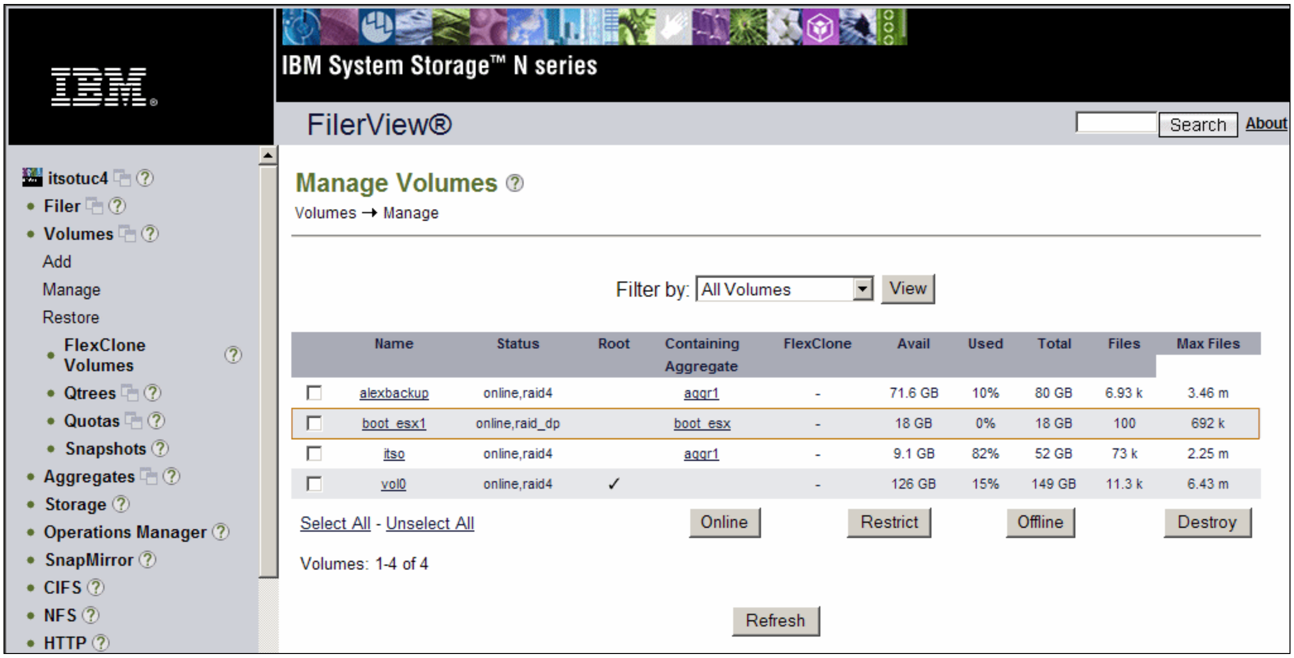



*Figure 5-19 New volume*

4. After you create the volume, add the LUN that is to be used by the VMware ESX Server as a bootable LUN:

   a. In the left pane of the FilerView panel, select **LUNs** → **Add**.

   b. In the Add LUN panel (Figure 5-20), complete the following actions:

      i. For Path, insert the path and the name of the LUN as follows:

         `/vol/<volume_name>/<lun_name>`

         In this example, we create a LUN named server1 in the volume named boot_esx1.

      ii. For LUN Protocol Type, select **VMware**.

      iii. For Description, enter a simple description for the new LUN.

      iv. For Size, enter the size of the LUN that is being created. In this example, we create a 7 GB LUN for the installation of the VMware ESX operating system.

      v. For Space Reserved, select the check box to allocate the new LUN the size that you chose in step iv.

      vi. Click the **Add** button.

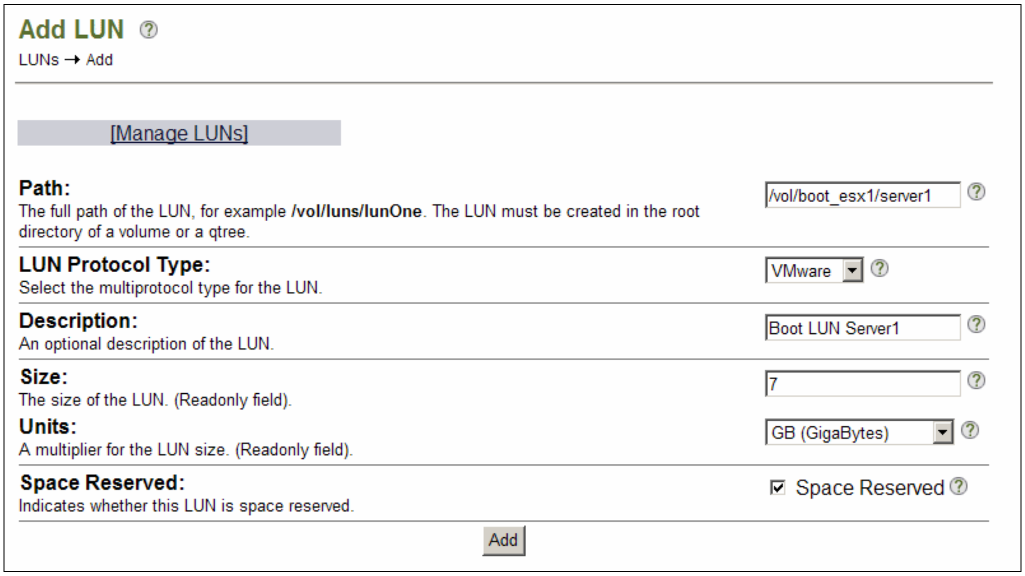



*Figure 5-20 Setting up the LUN to add*

c. To see the new LUN, in the left pane of the FilerView window (Figure 5-21), select **LUNs** → **Manage**. As shown in Figure 5-21, the LUN has no *mapping* assigned to it, meaning that the Fibre Channel HBA of the server is still unable to see this new LUN.

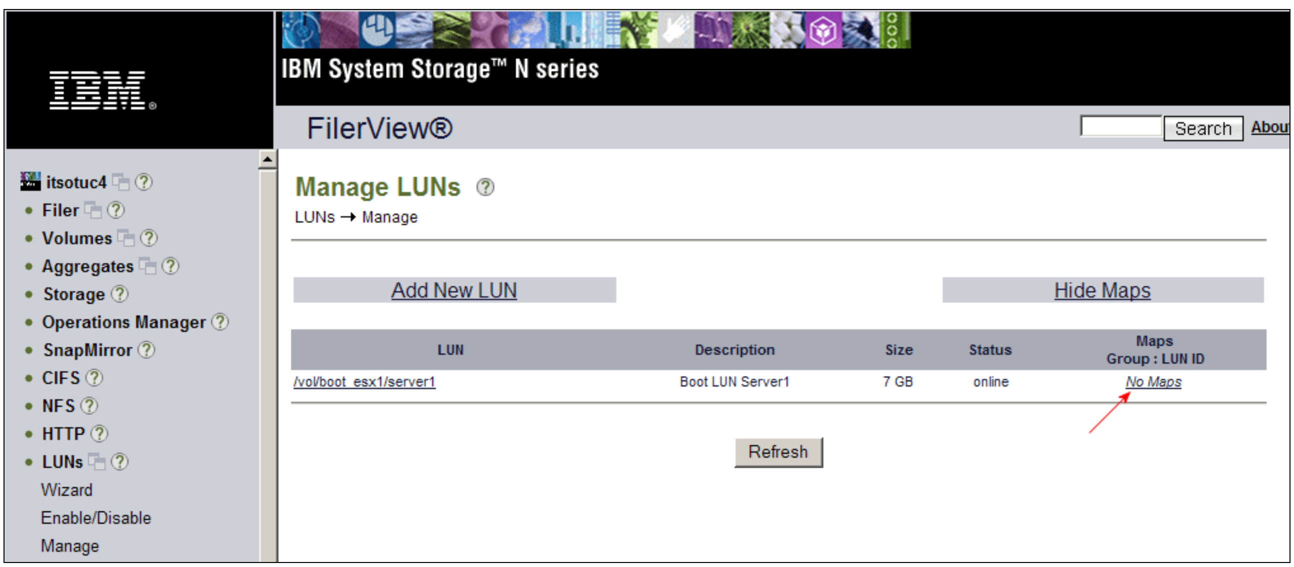



*Figure 5-21 New LUN without mapping*

5. To make the LUN available to the server's HBA, create an *initiator group* and add the WWPN of the server's HBA that must use this LUN.

   The WWPN is an identification number that every HBA integrates in its Basic Input/Output System (BIOS). This number is defined by the manufacturer and is unique. See 5.3.3, "Configuring Fibre Channel HBA for boot from SAN" on page 82, for information about obtaining the WWPN of the HBA and how to prepare the HBA to be a bootable device.

To create an initiator group, follow these steps:

a. In the left pane of the FilerView panel, select **Initiator Groups** → **Add**.

b. In the Add Initiator Group panel (Figure 5-22), complete these steps:

   i. For Group Name, specify the name of the initiator group.

   ii. For Type, select either **FCP** or **iSCSI**. In this example, we connect the storage system and the server through FCP and, therefore, select **FCP**.

   iii. For Operating System, select the VMware operating system that N series can recognize. Choose **VMware**.

   iv. For Initiator, list the WWPN of your HBAs.

   v. Click the **Add** button.

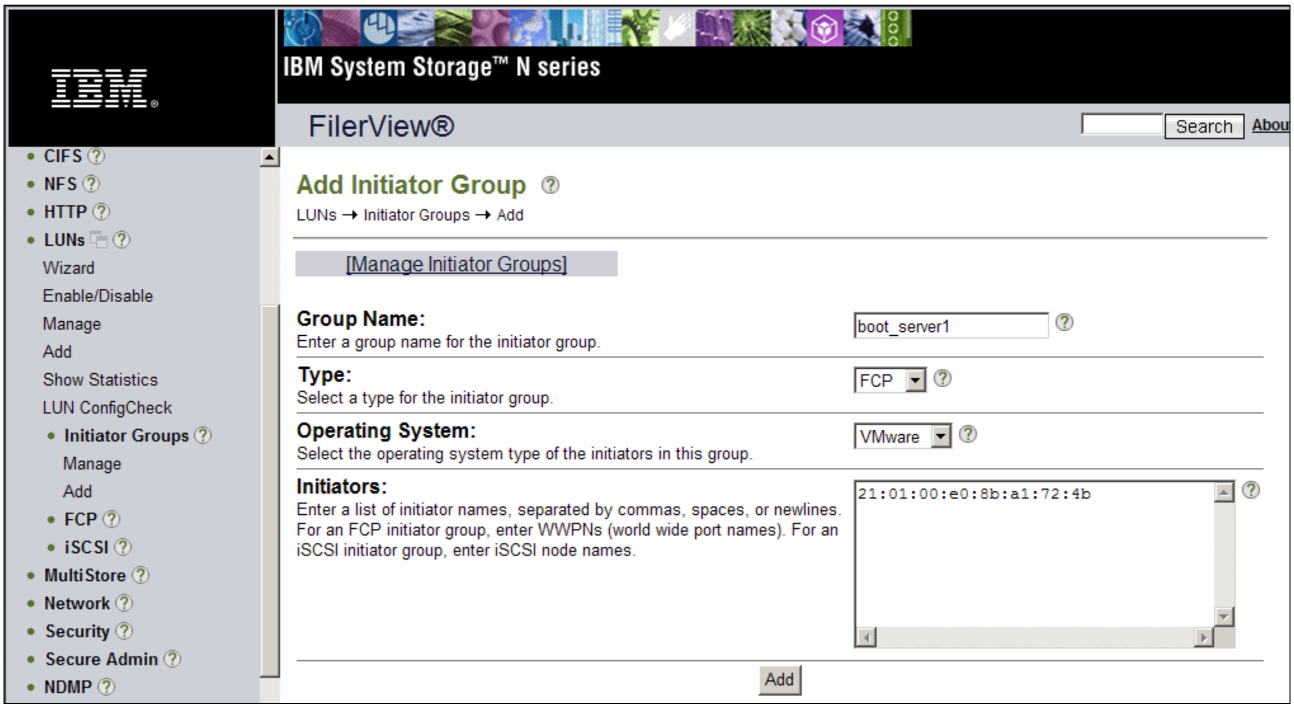



*Figure 5-22 Setting up the initiator group*

6. Map the LUN to the initiator group:

a. In the left pane of the FilerView panel, select **LUNs** → **Manage**.

b. In the Manage LUNs panel (Figure 5-23), click the LUN you created in step 4 on page 72 and then click the **No Maps** link.

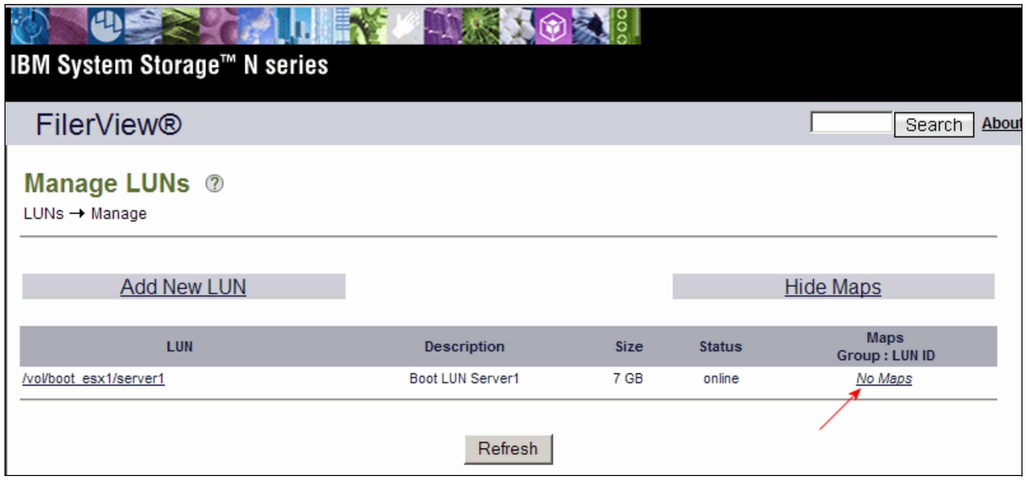



*Figure 5-23 Mapping the LUN: No maps link*

vi. In the LUN Map Add Groups panel (Figure 5-24), assign the initiator group that you created to the LUN. Then click **Add**.

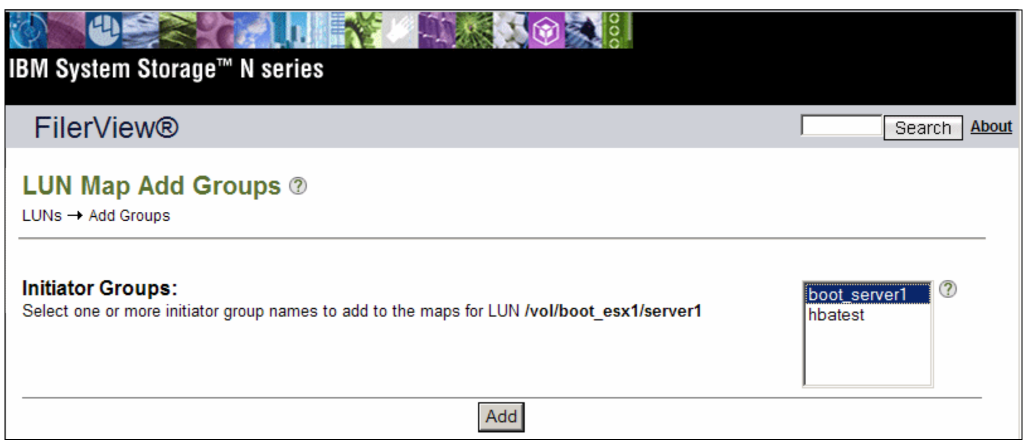



*Figure 5-24 Assigning the initiator group to the LUN*

c. In the LUN Map panel (Figure 5-25), give the LUN an ID. In the LUN ID box, type 0 and then click **Apply**.

> **Important:** The LUN ID of the bootable LUN must always be set to 0, or the LUN cannot boot.

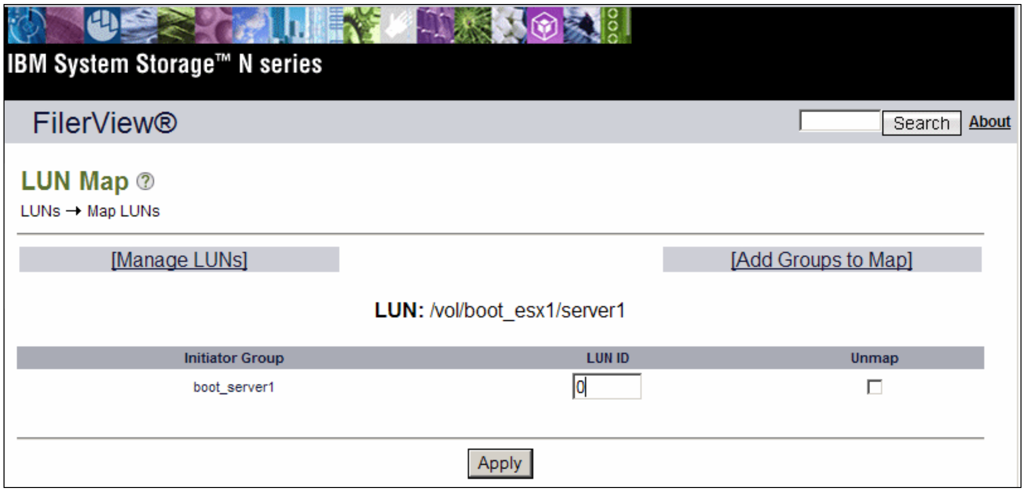



*Figure 5-25 Giving the LUN an ID*

d. To see the LUN, in the left pane, select **LUNs** → **Manage**, as shown in Figure 5-26.


*Figure 5-26 Viewing the new LUN*

## 5.3.2 Zoning a LUN in the SAN switch

Because the connection of a bootable LUN for the VMware ESX operation system must go through a SAN switch, you must properly zone the bootable LUN to the server's HBA:

1. Launch an Internet browser and type the following URL:

   `http://<SAN_switch_address>`

   Where *SAN_Switch_address* is the name or IP address of your SAN switch system.

2. In the main window, click the **Zone menu** icon at the bottom of the window (circled in Figure 5-27).

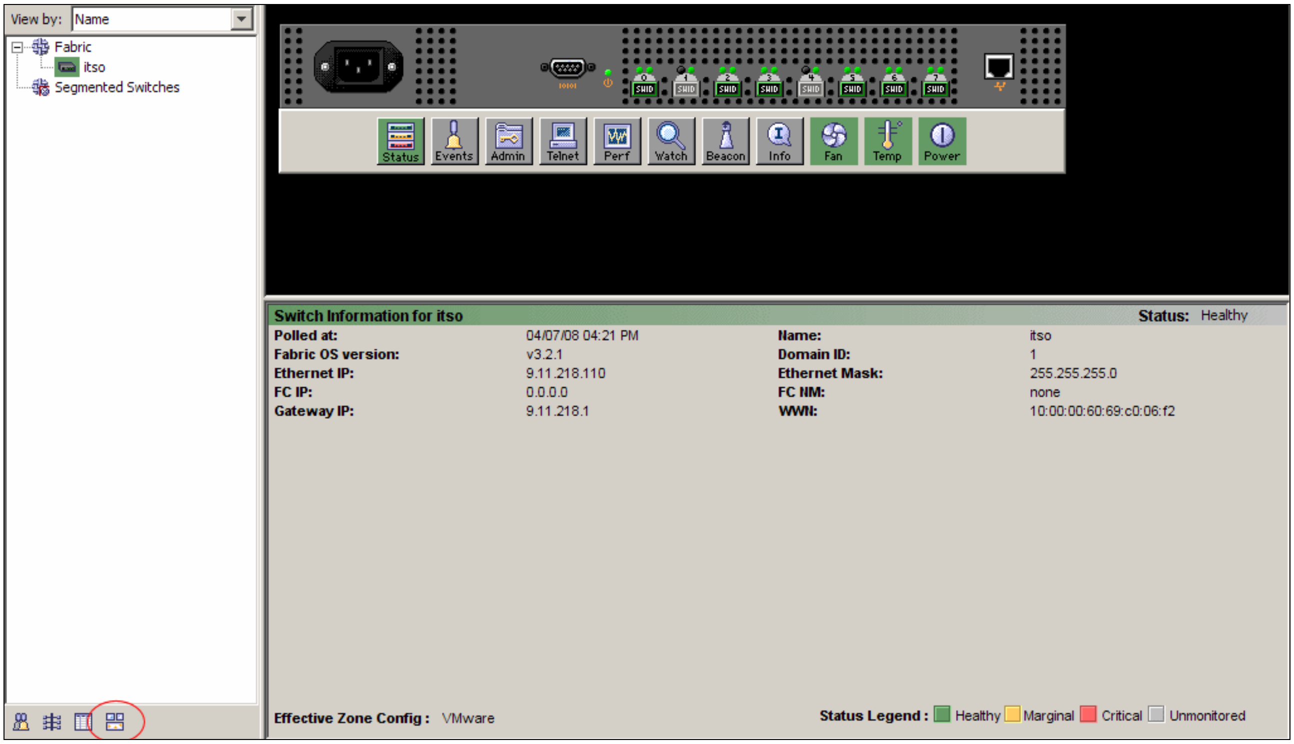



*Figure 5-27 Clicking the Zone menu icon*

3. When prompted, enter your user name and password to access the zoning feature of the SAN switch, as shown in Figure 5-28. Then click **OK**.

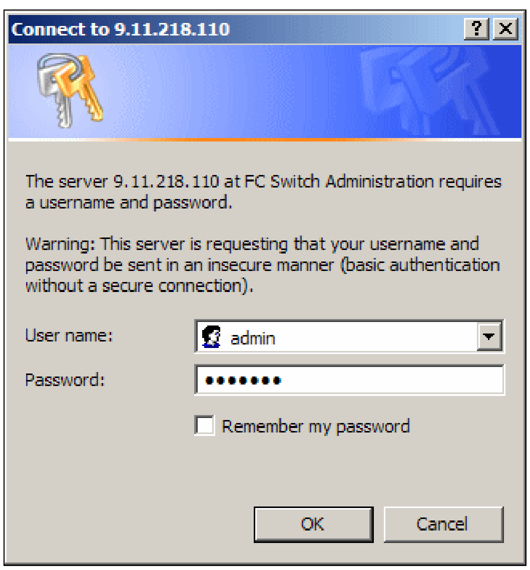



*Figure 5-28 Signing on to access the zoning feature of the SAN switch*

4. In the LUN zoning window (Figure 5-29), on the **Zone** tab, click the **Create** button to add a new zone.

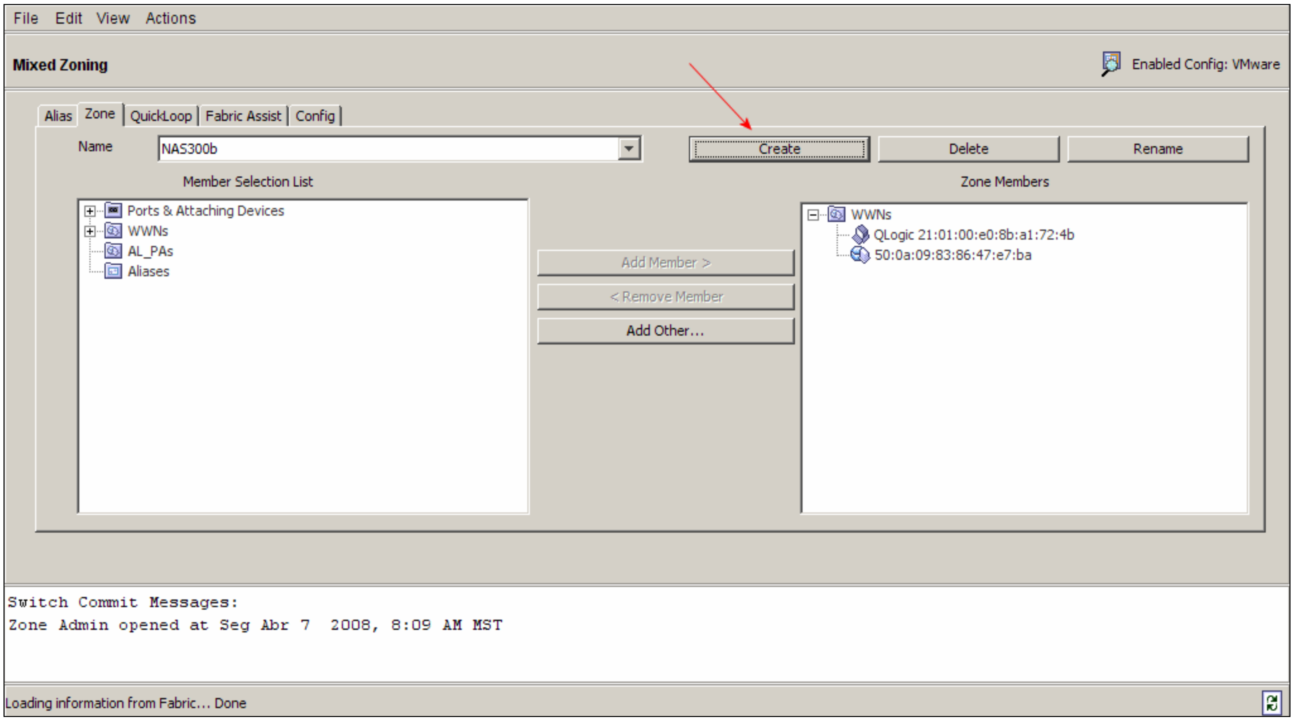



*Figure 5-29 Creating a new zone*

a. In the Create New Zone window (Figure 5-30), give the new zone a name. In this example, we name it boot_server1. Then click **OK**.

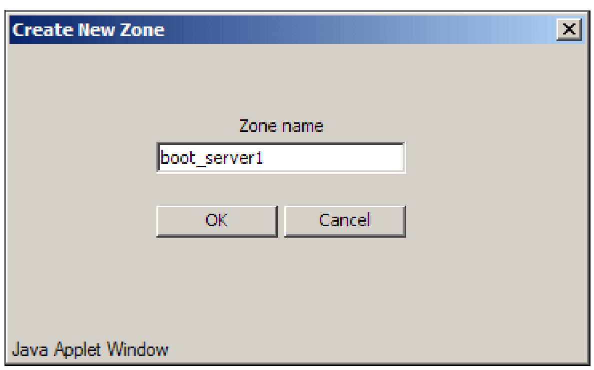



*Figure 5-30 Naming the new zone*

b. Assign the proper WWPNs of the storage system and the server's HBA to the new zone (Figure 5-31):

   i. From the Name list, select the proper zone name.

   ii. Expand the **WWPN** menu to see your storage and server's WWPNs, and select each of them.

   iii. Click the **Add Members** button.

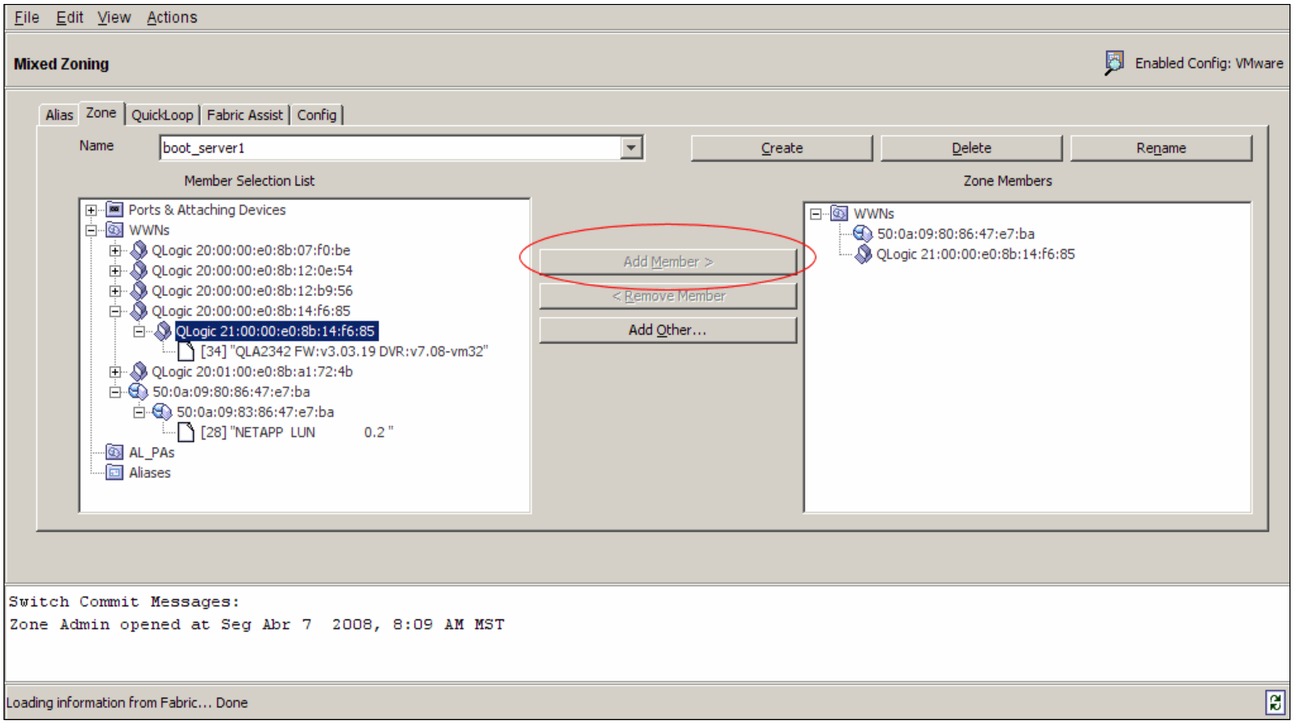



*Figure 5-31 Assigning the WWPNs of the storage system and server HBA to the zone*

5. Click the **Config** tab (Figure 5-32) and add the zone named boot_server1 to the switch configuration. This example has a switch configuration named *VMware*. Click the proper zone name and then click the **Add Members** button.

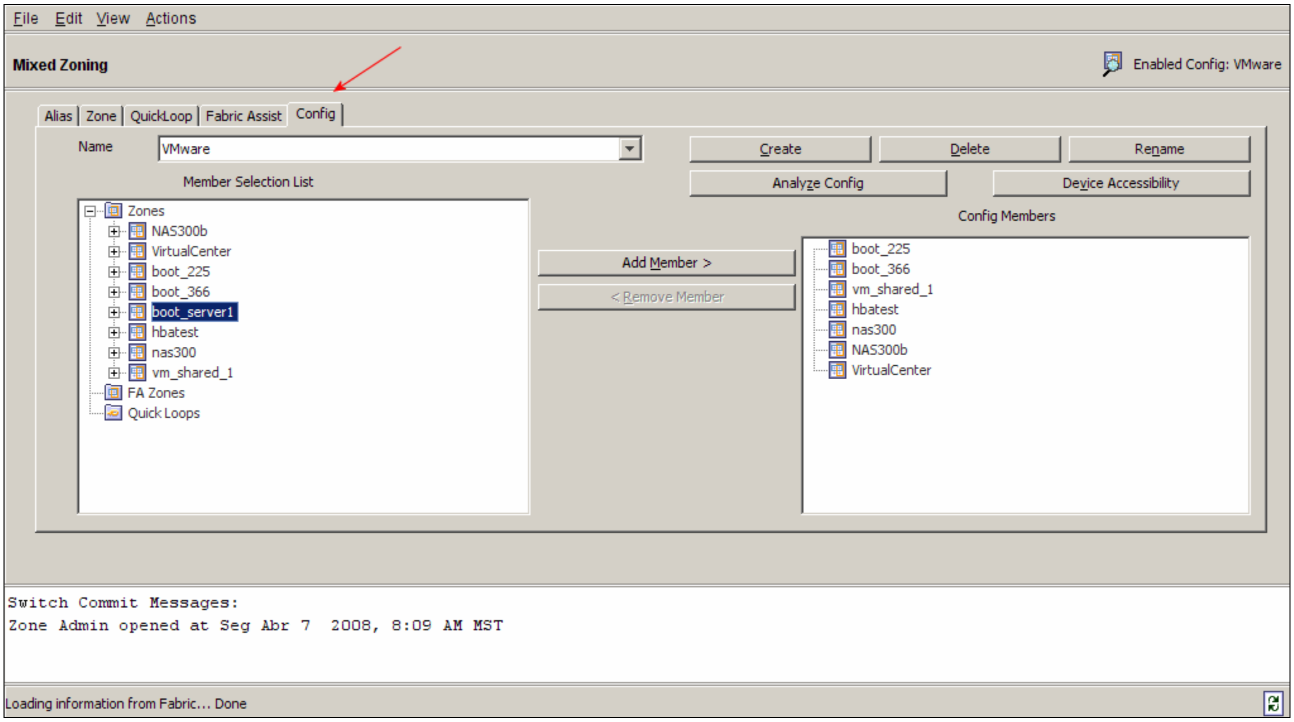



*Figure 5-32 Adding members to the switch configuration*

6. To deliver the LUN to the server and make it available, complete these steps:

   a. Select **Actions** → **Enable Config** to enable the SAN switch configuration with the new zone as shown in Figure 5-33.

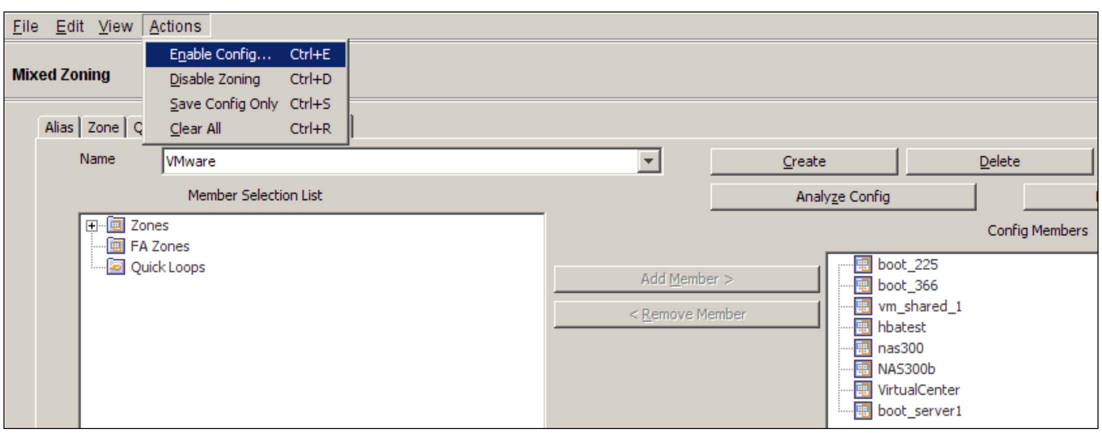



*Figure 5-33 Enabling the SAN switch configuration*

b. In the Enable Config window (Figure 5-34), select the configuration to enable. In this example, we select **VMware** configuration. Click **OK**.

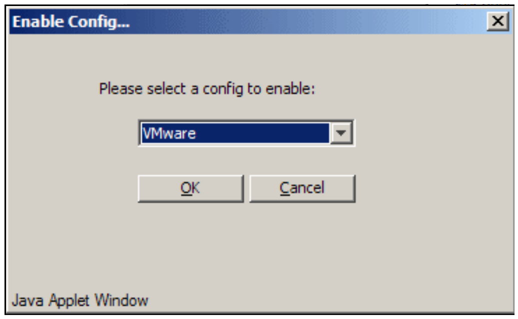



*Figure 5-34 LUN zoning - enable configuration selection*

c. In the Enable Config VMware message box (Figure 5-35), click **Yes**.

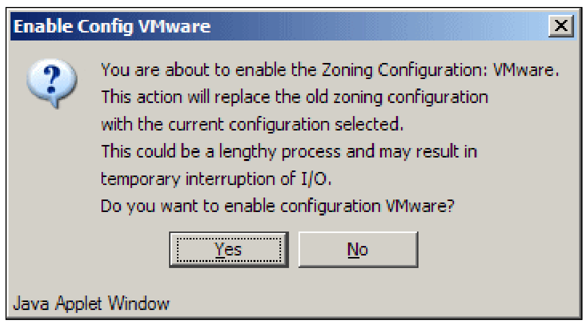



*Figure 5-35 Replacing the SAN switch configuration*

Figure 5-36 shows the log section is at the bottom of the window. You can make sure that the SAN switch configuration was enabled successfully when the log message `Commit Succeeded` is shown. The server can now use this LUN.

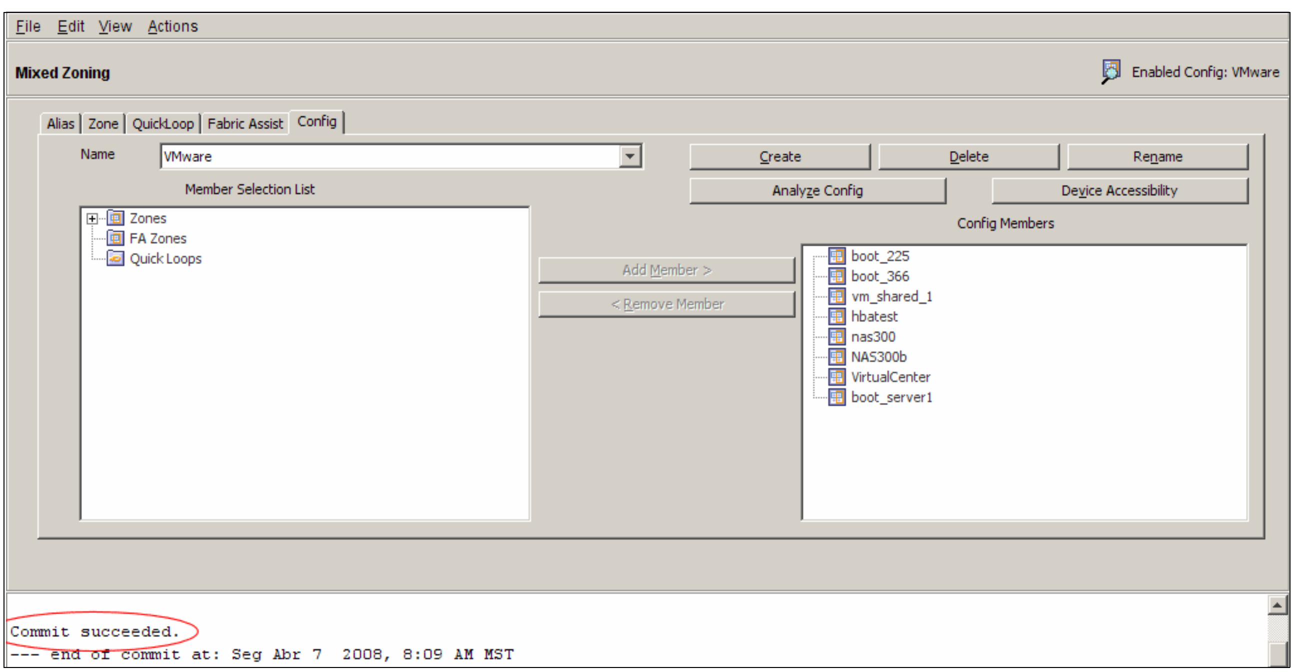



*Figure 5-36 LUN zoning - commit SAN zone changes*

## 5.3.3 Configuring Fibre Channel HBA for boot from SAN

Now that you have created the LUN of the VMware operating system and zoned it to the server, configure the HBA device of the server as a bootable device.

> **EMULEX HBAs:** This example shows how to configure a QLogic HBA as a boot device. For EMULEX HBAs, see the QLogic documentation at:
>
> `http://filedownloads.qlogic.com/files/manual/69771/FC0054606-00.pdf`

### Configuring the QLogic HBA

To configure the QLogic HBA, follow these steps:

1. Boot the server and, during the post, press Ctrl-Q to enter the QLogic BIOS (Figure 5-37).

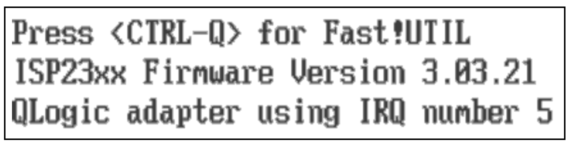



*Figure 5-37 HBA setup - step 1*

2. Select the HBA to be used (if more than one is available) and press Enter.
3. In the Fast!UTIL Options panel (Figure 3), use the arrows keys to highlight the **Configuration Settings** option and press Enter.

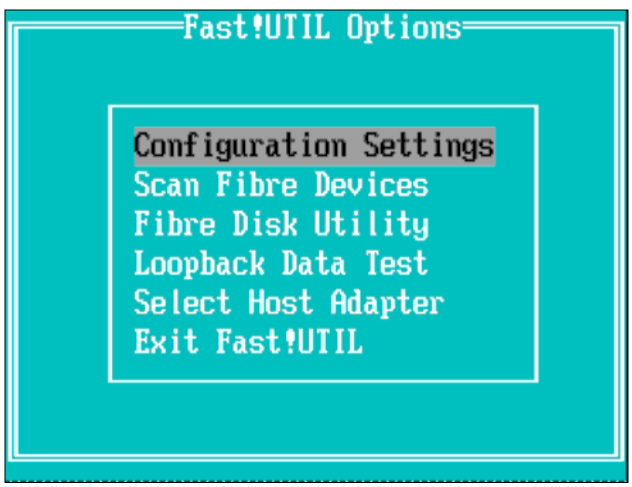



*Figure 5-38 Selecting the Configuration Settings option*

4. In the Configuration Settings panel (Figure 5-39), select **Adapter Settings** and press Enter.

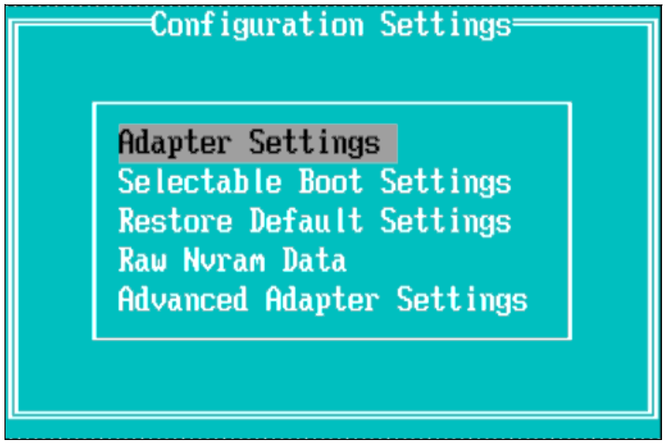



*Figure 5-39 Selecting the Adapter Settings option*

5. In the Adapter Settings panel (Figure 5-40), for Host Adapter BIOS, change the value to **Enabled**. You can also see the WWPN of the HBA in the Adapter Port Name field. Press Esc to exit this page.

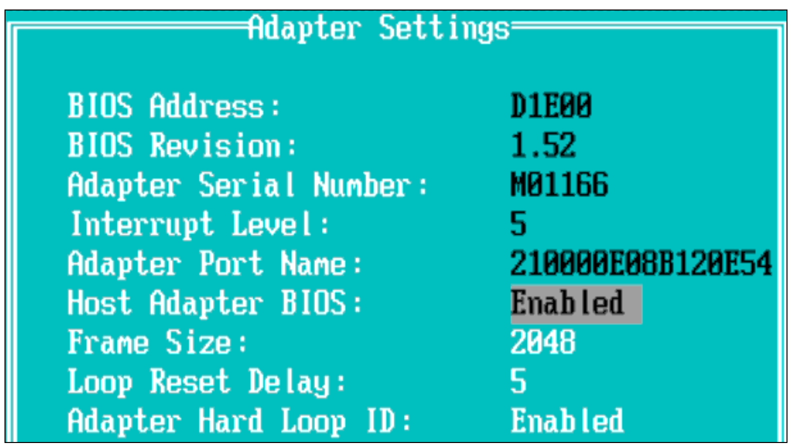



*Figure 5-40 Enabling Host Adapter BIOS*

6. In the Configuration Settings panel (Figure 5-39), select the **Selectable boot settings** option and press Enter.

7. In the Selectable Boot Settings panel (Figure 5-41), highlight the **Selectable Boot** option and change it to **Enable**.

   In this same panel, you can see the WWPN of your HBA; highlight it and press Enter.

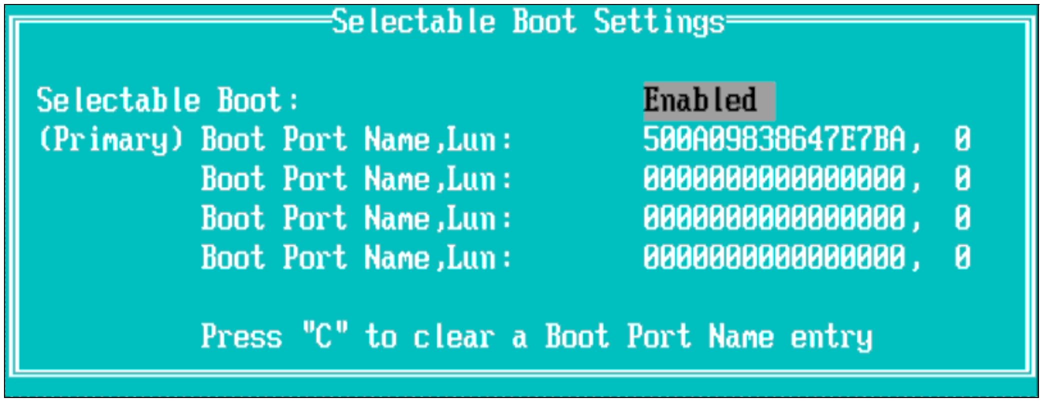



*Figure 5-41 Enabling Selectable Boot*

8. Now that the HBA is ready to be a bootable device, press the Esc key and choose the option **Reboot Server** (Figure 5-42).


*Figure 5-42 HBA setup*

## Configuring the boot sequence

If the server has internal disks, you can configure the HBA device with a higher priority in the server's boot sequence. You enter the BIOS settings of your server and configure the boot sequence to make the CD drive the first boot device and the HBA the second boot device.

This example shows how to configure the boot sequence in BIOS Version 1.09 of an IBM System x3850 server.

**HBA:** Depending on your version of the BIOS, the HBA is referred to as *Hard Disk 0* and not as the HBA itself.

Follow these steps:

1. During the post of the server, press F1 to go to the system BIOS.
2. In the Configuration/Setup Utility panel (Figure 5-43), use the arrow keys to highlight **Start Options**. Press Enter.

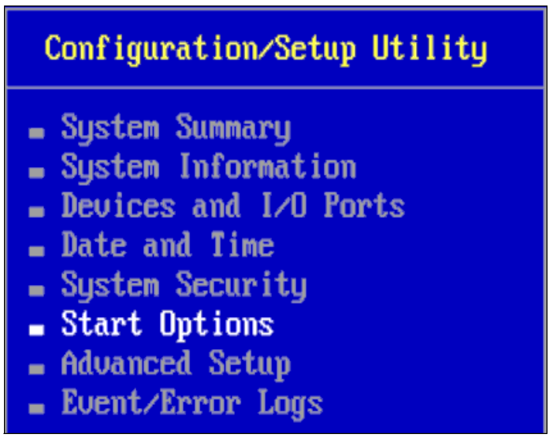



*Figure 5-43 Selecting Start Options*

3. In the Start Options panel (Figure 5-44), select **Startup Sequence Options** and press Enter.


*Figure 5-44 Selecting Startup Sequence Options*

4. In the Startup Sequence Options panel (Figure 5-45), for First Startup Device, type `CD ROM`, and for Second Startup Device, type `Hard Disk 0`. Press Esc to return.

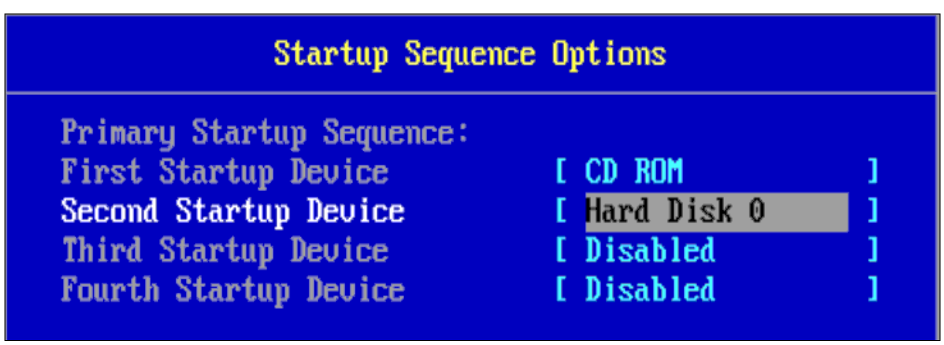



*Figure 5-45 Specifying the first and second startup devices*

5. In the Exit Setup window, as in Figure 5-46, select **Yes, save and exit the Setup Utility**.

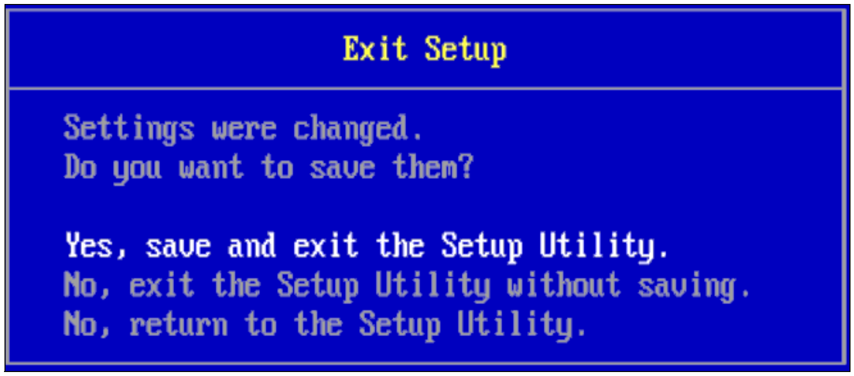



*Figure 5-46 Saving the changes and exiting the Setup Utility*

6. Reboot the server.

The server and LUN are ready for the ESX operating system installation.

## 5.4 Installing the ESXi operating system

To install the ESXi operating system, follow these steps:

1. Insert the ESXi operating system installation CD into the CD tray or mount the ISO image if you are using a remote card
2. When prompted to select the installation mode, as in Figure 5-47, choose either the graphical (GUI) or text interface. Press Enter to choose the GUI.

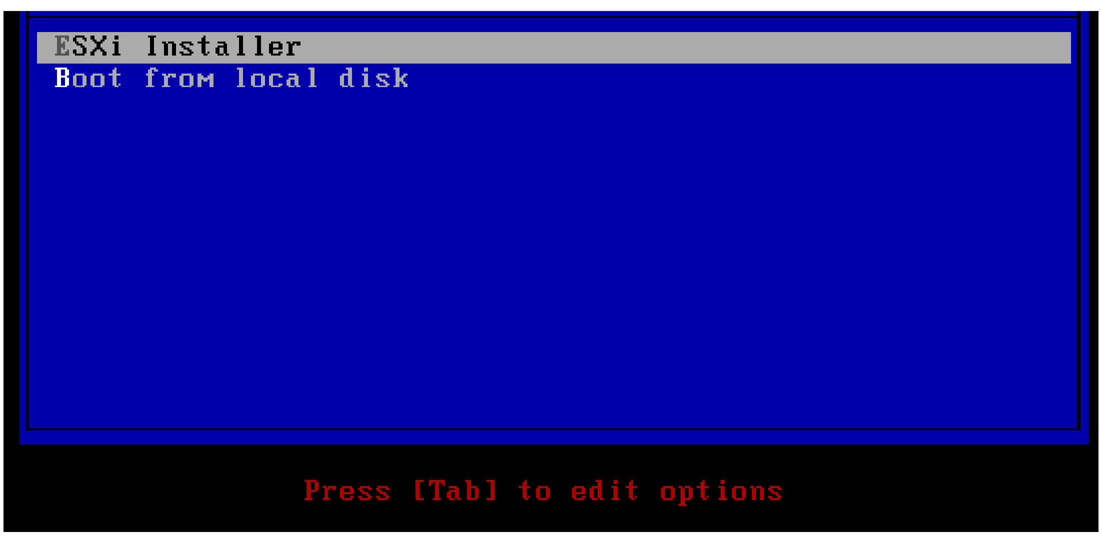



*Figure 5-47 Choosing the ESXi installation mode*

The installer loads the necessary drivers (such as HBA and network card drivers) for the operating system installation.

3. After the media test is successfully completed and the installation wizard starts, in the Welcome window in Figure 5-48, click **Next**.

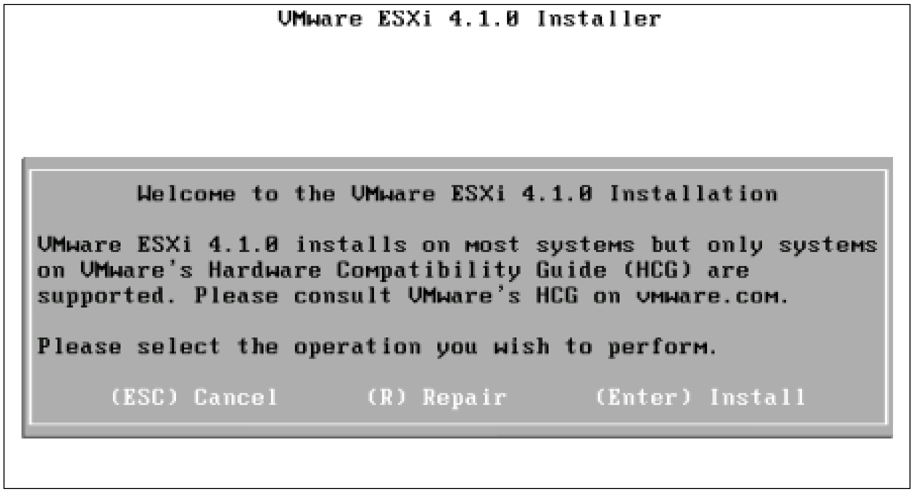



*Figure 5-48 ESXi 4.1 Welcome window*

4. In the license agreement panel, in Figure 5-49, read the license text. If you agree with the terms, press F11 to proceed with the installation.

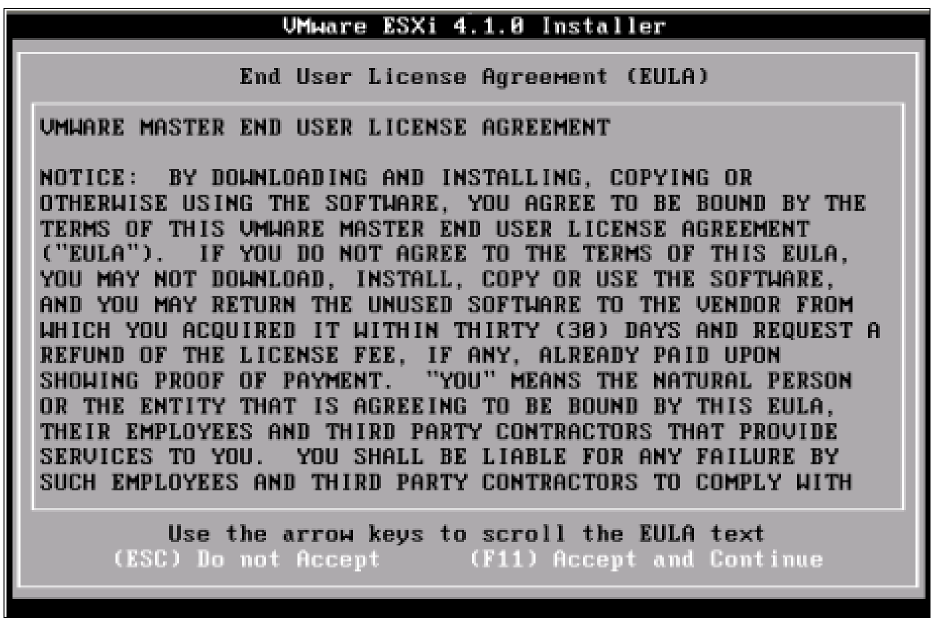



*Figure 5-49 License agreement panel*

5. In the next step, shown in Figure 5-50, VMWare list the physical disks found during its scanning. Those disks include local ones and LUNs provided to be used by SAN boot systems panel (choose how you want to set up the initial system partition).

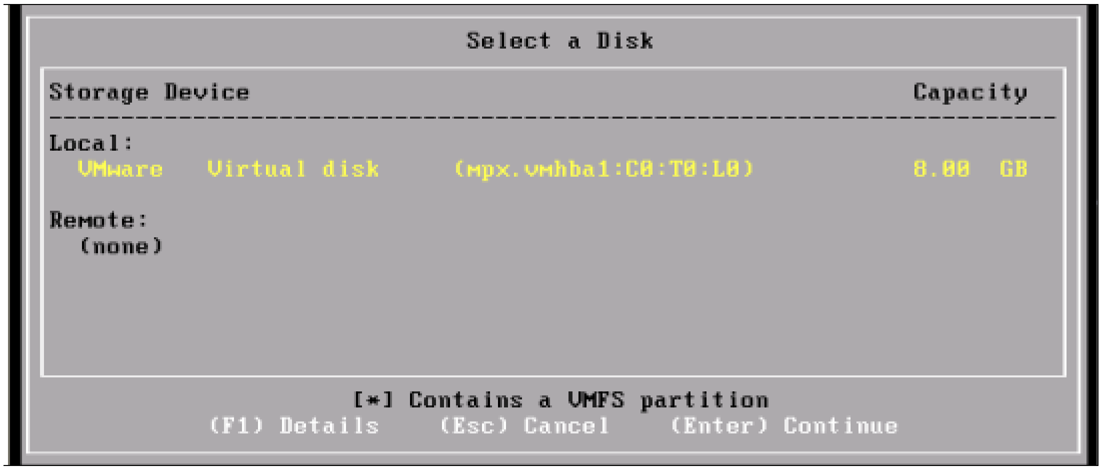



*Figure 5-50 Selecting the disk to install ESXi 4.1*

6. The next panel, in Figure 5-51, shows the confirmation install.

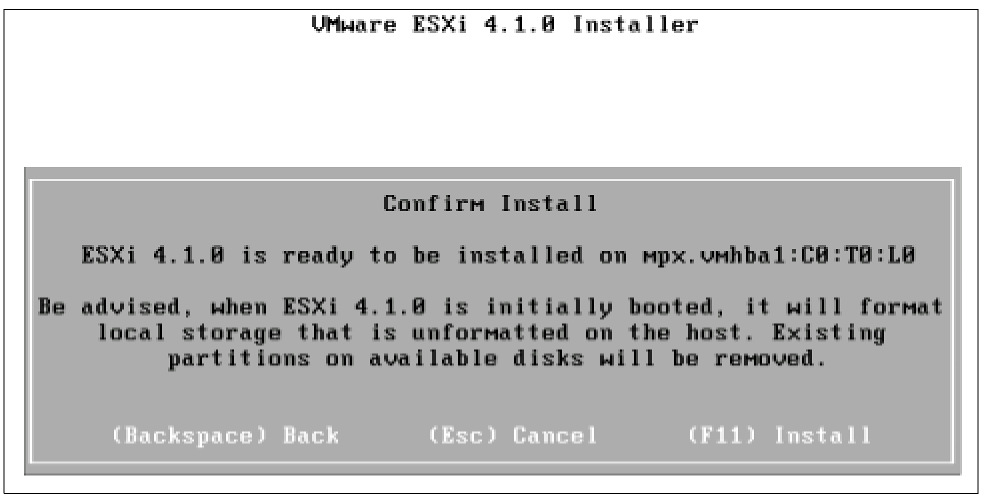



*Figure 5-51 Installer waiting the confirmation to start installation (F11)*

7. The installation takes few minutes and finishes successfully as in Figure 5-52).


*Figure 5-52 Installation completed*

8. Remove the CD or unmount the ISO, then restart the server, and you have the following panel, as in Figure 5-55.

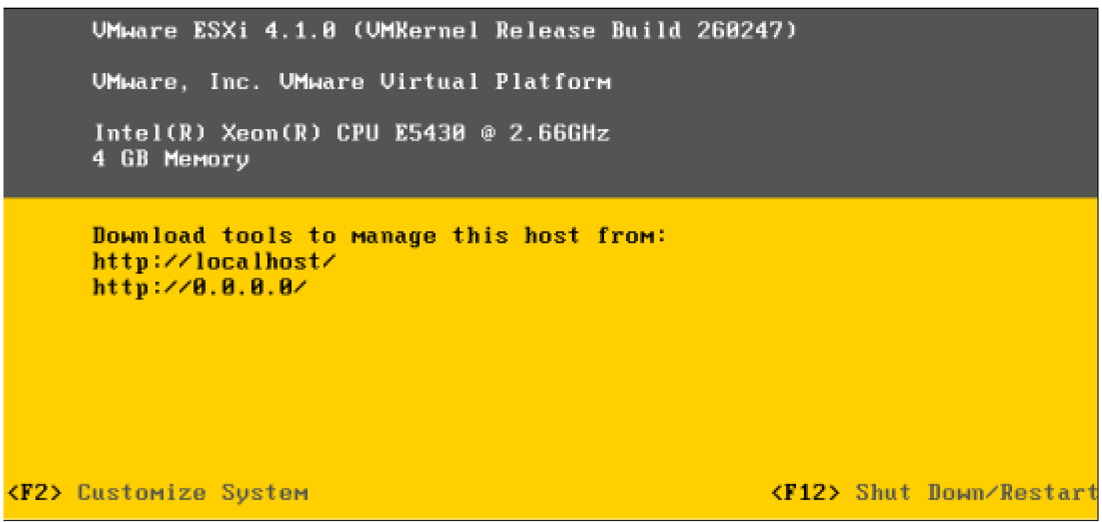



*Figure 5-53 Fresh installed ESXi 4.1*

9. Press F2 to customize the server, then enter the root password as shown in Figure 5-54, which is empty by default, so just press Enter.


*Figure 5-54 Login to the ESXi host*

10. The first highlighted option is **Configure Password**, so press Enter to set it.

11. Type it twice on the next panel and press Enter again.

12. Then go to the **Configure Management Network** option, press Enter, select **IP Configuration**, and press Enter again. Then configure the host with your networking settings, as in Figure 5-55.

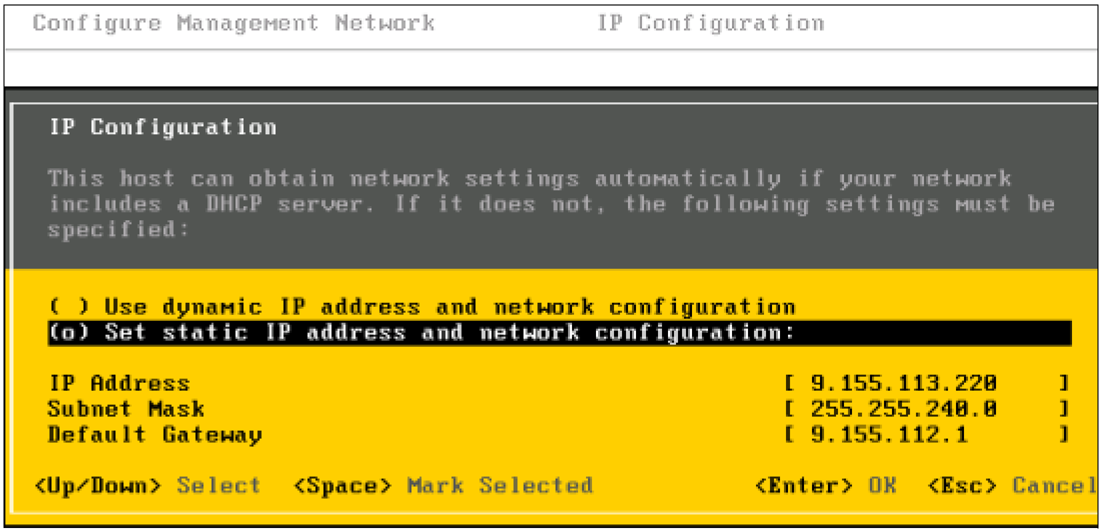



*Figure 5-55 Setting network information on the host*

13. After setting the network, press Enter, go to **DNS configuration**, and press Enter. Type the network information and the hostname of the server, as in Figure 13, and press Enter.


*Figure 5-56 Set the DNS servers and the Hostname*

14. Press Esc to leave the Configure Management Network, and on the confirmation panel, select **Y**, as in Figure 5-57.


*Figure 5-57 Restarting the management network to apply changes*

15. Connect the host to a vCenter and apply all the available patches.

16. Take a backup of your host configuration by using vSphere CLI, running the following command:

```
vicfg-cfgbackup --server <ESXi-host-ip> --portnumber <port_number> --protocol
<protocol_type> --username username --password <password> -s <backup-filename>
```

.Use the -s option to point the location where the file with the host configuration is intended to be saved.

# 6

# Installing and configuring VMware vCenter 4.1

This chapter provides information about how to install and configure VMware vCenter and perform basic administration activities. It includes the following topics:

- VMware vCenter 4.1 overview
- Installing VMware vCenter 4.1
- Basic administration with VMware vCenter

## 6.1 VMware vCenter 4.1 overview

VMware vCenter is a central console that enables the most valuable virtualization features. These features include vMotion, High Availability (HA), Distributed Resource Scheduler (DRS), Storage vMotion, Fault Tolerance (FT), and Cloning, to name only the most common.

It is implemented as a service running on a Windows server. On vCenter 4.1, it requires a 64-bit operating system. So, if you are installing a server to perform that role, ensure that it can run a 64-bit OS. Some examples include Windows 2003 64-bit on any version (Standard, Enterprise, or Datacenter), Windows 2008 64-bit on any version, or Windows 2008 R2.

VMware vCenter uses a database to store all the configuration of its elements, such as hosts, virtual machines, datastores, and clusters. When installing a small environment (up to five hosts), it is acceptable to use a light version of Microsoft SQL Server or IBM DB2. These versions are free but have limited capacities. For larger environments, use of a full database bundle is required.

For more information about compatibility, requirements, patch level and specific configuration, check the *ESXi Installable and vCenter Server Setup Guide*, at the following website:

http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esxi_i_vc_setup_guide.pdf

Because our environment has less than five hosts, we use SQL 2005 Express, which is included on the VMware vSphere installation image.

For management purposes and authentication separation from the OS, we created a user (which we named VCadmin) to run the vCenter Server service. This user must be an administrator of the server where vCenter is intended to run.

## 6.2 Installing VMware vCenter 4.1

In this book, we are using VMware vCenter version 4.1 Update 1. We consider that you have a VMware registration with enough rights to perform that task. To install it, perform the following steps:

1. Mount the vCenter installation image with your preferred image software.
2. If the autorun loads the installation panel, close it. Browse the image, right-click the file autorun.exe while holding the Shift key, and select **Run as different user**, as shown in Figure 6-1.

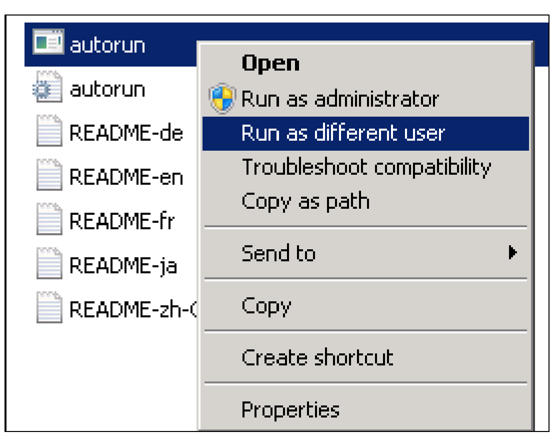



*Figure 6-1 Running the installer as a different user*

3. Type the credentials and click **OK**.
4. When the installation panel is displayed, select vCenter Server, as in Figure 6-2.

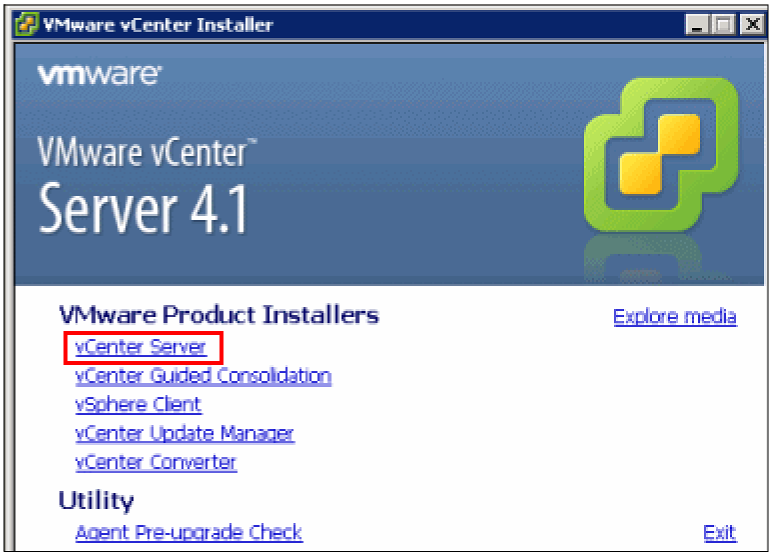



*Figure 6-2 Selecting vCenter to be installed*

5. Select the language that you are going to use and click **OK**.
6. Click **Next** on the Welcome panel.
7. Click **Next** on the End-User Patent Agreement panel.
8. In the License Agreement, change the radio button to "*I agree to the terms in the license agreement*" and click **Next**.
9. In the next panel, enter your company information and the vCenter Server license. You can type it later also, which sets it to evaluation mode of 60 days. Click **Next**.
10. On Database Options, choose between the included version of SQL for small deployments or "*Use an existing supported database* ". We are going the use the SQL Express, as in Figure 6-3, but in a real environment, use a full bundle database. Click **Next**.

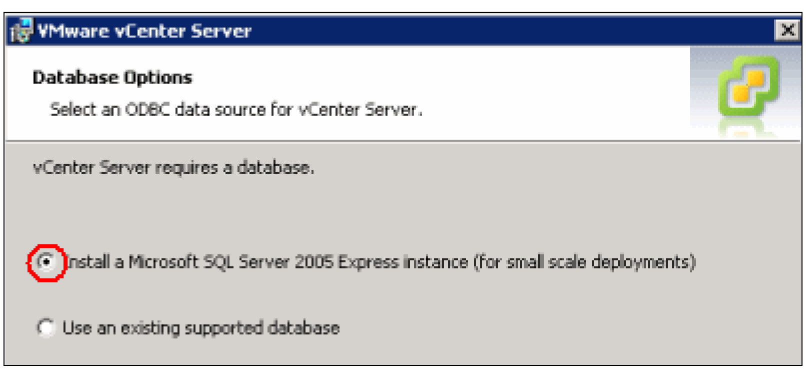



*Figure 6-3 Selecting the database*

> **Attention:** The DSN (Database Source Name) must be 64-bit capable. Otherwise, it does not work.

11. Because the installation was started with the VCadmin user, it is the one intended to run the vCenter Server service (see Figure 6-4). Type its password and click **Next**.

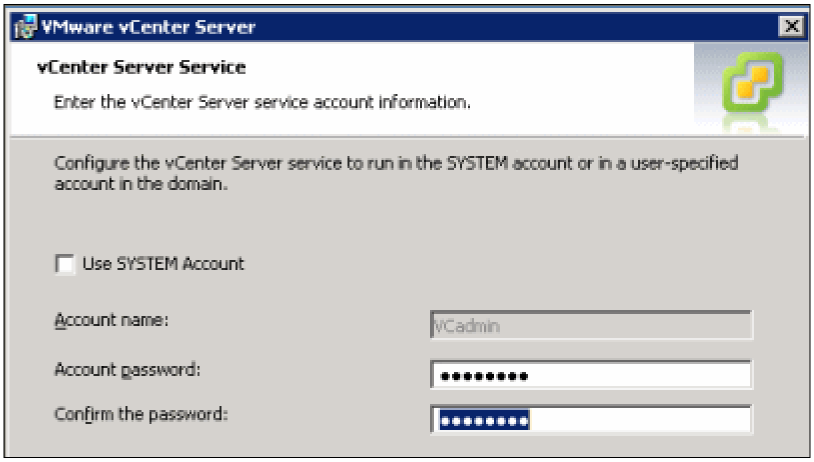



*Figure 6-4 vCenter account during the installation*

12. To facilitate administration, it is a best practice to keep the OS data separated from the application. So we install vCenter on another partition, as shown in Figure 6-5, and click **Next**.

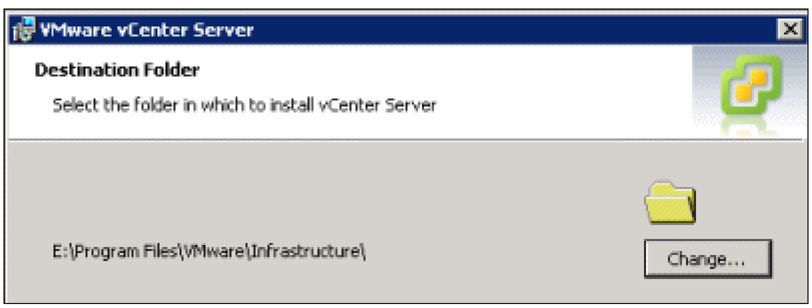



*Figure 6-5 Installing vCenter in a different partition than the OS*

13.Because this vCenter is the first one of the structure, it must be a stand-alone instance, as shown in Figure 6-6. (If it happens to be the second or any other, we can install it as linked to the first instance, which is called a Linked Mode instance.) Click **Next**.

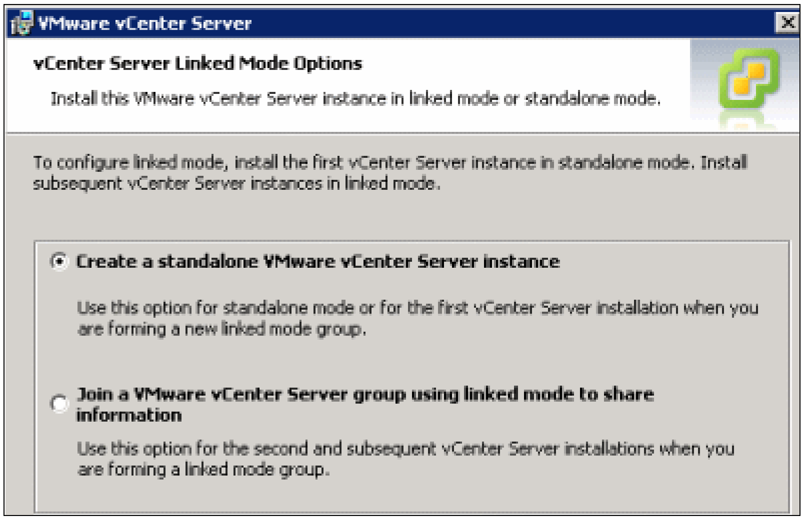



*Figure 6-6 Creating a stand-alone instance*

14.On the Configure Ports panel, leave the default ports if they not in conflict with any application that you can have on the vCenter server. Click **Next**.

> **Important:** vCenter uses ports 80 and 443. So if you are installing it over a web server, you must change those ports when installing vCenter to change your web server configuration. Otherwise, the vCenter Server service fails to start.

15.On the vCenter Server JVM Memory panel, select the option that best describes your environment according the number of hosts you are intending to run. Then click **Next**.

16.On the Ready to Install the Program, click **Install** to start the installation.

## 6.3 Basic administration with VMware vCenter

This section explains how to perform a basic configuration of vCenter for a quick start. For more details, see the VMware *Datacenter Administration Guide* at the following website:

http://www.vmware.com/pdf/vsphere4/r41/vsp_41_dc_admin_guide.pdf

This topic includes the following sections:

- Creating a datacenter
- Creating a cluster
- Adding hosts to a cluster
- Templates

## 6.3.1 Creating a datacenter

To perform a basic configuration in vCenter, create a datacenter object to group the other objects created below it:

1. Open vCenter and log in.
2. Right-click the vCenter object and select **New Datacenter**, as in Figure 6-7. Set its name accordingly.

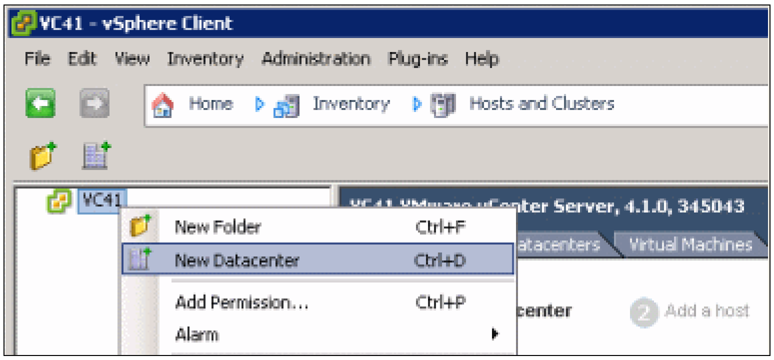



*Figure 6-7 Creating a Datacenter*

## 6.3.2 Creating a cluster

A cluster is an entity which defines the boundaries of actions of both HA and DRS, so only the hosts and virtual machines included on clusters take advantage of those features.

To create a clone:

1. Right-click the Datacenter object, then select **New Cluster...** , as shown in Figure 6-8.

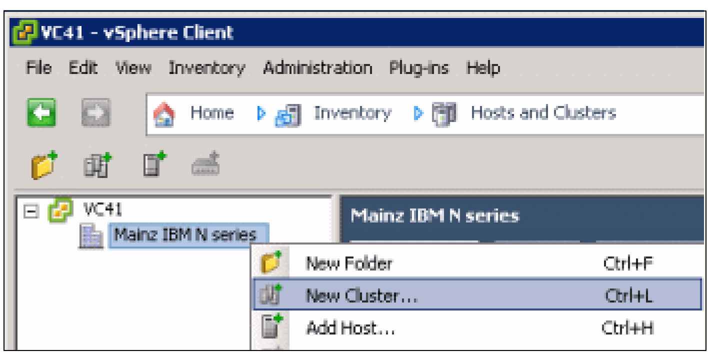



*Figure 6-8 Creating a new cluster*

2. On the next panel, provide a name to the cluster as in Figure 6-9. Select the options related to HA and DRS if you want to implement those features. Then click **Next**.

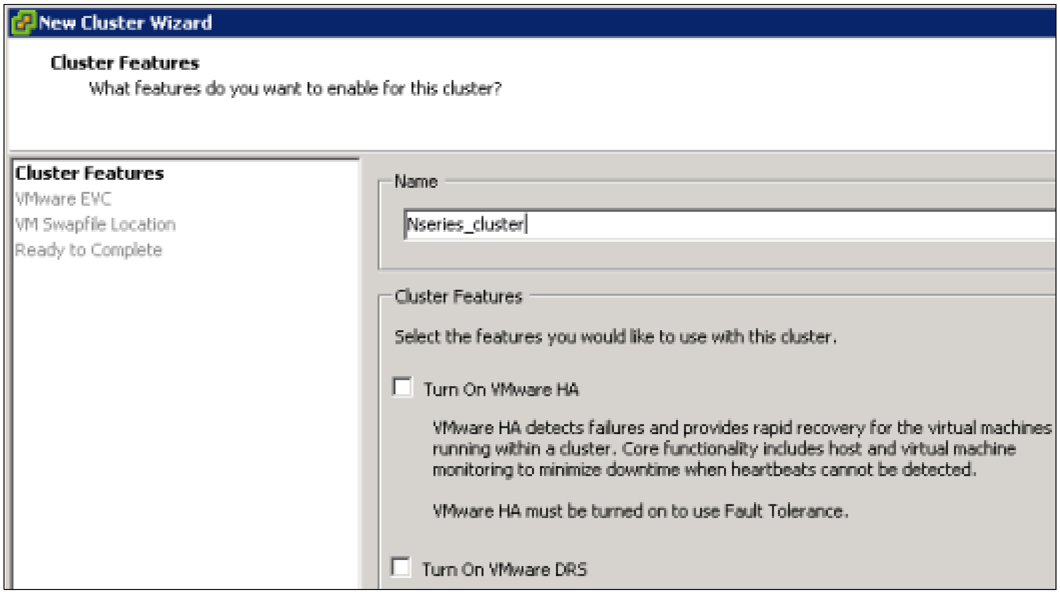



*Figure 6-9 Naming the cluster and features available: HA and DRS*

3. On the VMware EVC panel, whenever possible, enable EVC to facilitate vMotion between hosts with a slightly different version of processors, as shown in Figure 6-10. Click **Next**.

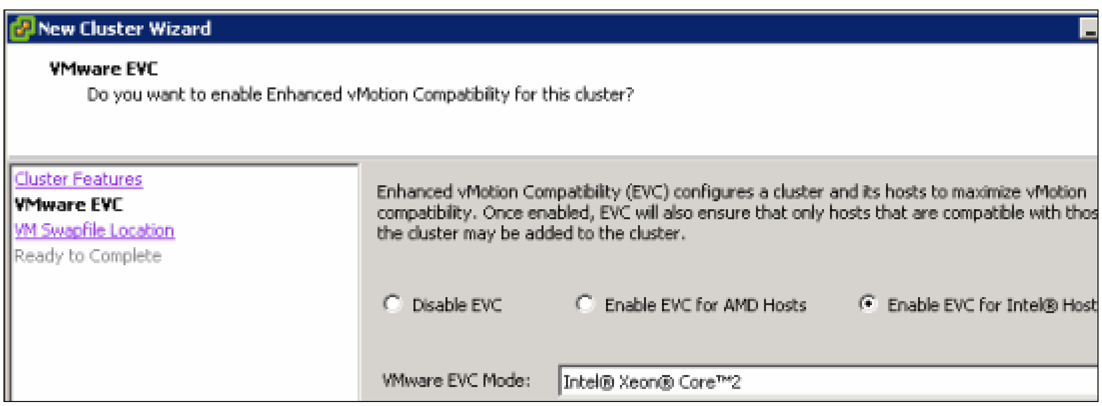



*Figure 6-10 Enabling EVC*

4. Select to leave the pagefiles in the same directory as the virtual machine for ease of management and recovery of them. Click **Next**.
5. Review the information and click **Finish**.

## 6.3.3 Adding hosts to a cluster

Before adding a host, you must have an ESX or ESXi host already installed and set up in the network. For more information about this task, see Chapter 5, “Installing the VMware ESXi 4.1 using N series storage” on page 61.

> **Tip:** Create a manual entry on your DNS zone for your ESXi hosts, because they do not create that automatically.

**Important:** Ensure that your DNS infrastructure is working correctly before adding servers to vCenter. If DNS cannot resolve the hosts, HA service can be affected.

After you set up the host, add it as follows:

1. As in Figure 6-11, right-click the cluster you want, and select **Add Host**...

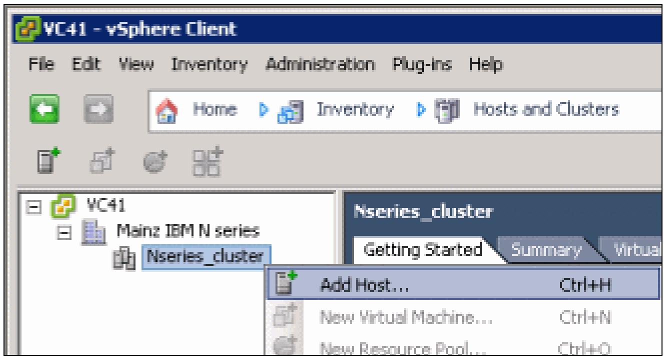



*Figure 6-11 Adding a host to a cluster*

2. Type the host's full qualified domain name, then root user, and its password, in the authentication box, as in Figure 6-12.

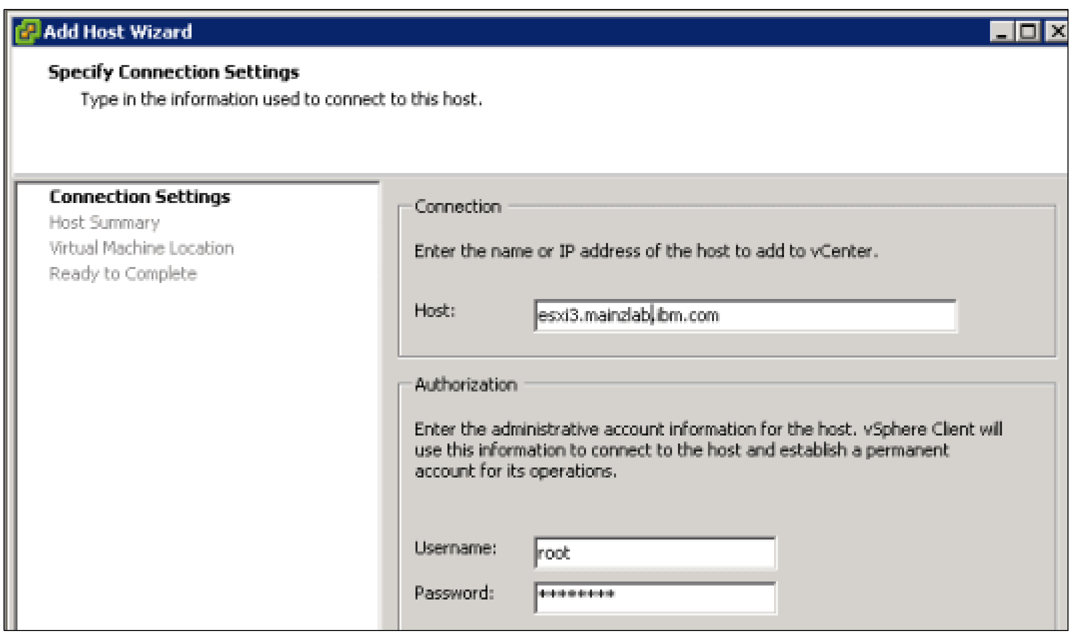



*Figure 6-12 Adding the host name, root user, and its password*

3. Accept the RSA key by clicking **OK**.
4. Select a placeholder where you want to store the virtual machines and click **Next**. The purpose here is for ease of administration only. You can create folders to divide the VM structure, as Windows and Linux VMs, or divide them by tier of applications. It really depends on your design.
5. In the Ready to Complete panel, review the information and click **Finish**.

## 6.3.4 Templates

A *template* is an image of a virtual machine (VM). You want to ease the administration and deployment of new VMs. So you generally install the operating system on the template image with all the basic software features that do not require special configuration, such as antivirus. A template is useful when you need to quickly deploy a large number of guests. You need only to set up a single guest and load its operating system, while the other machines are created as copies from that template.

**Prerequisites:** Before creating a template, it is a good idea to perform the disk block alignment before you load the operating system into the guest. For more information, see 7.9, "Partition alignment" on page 136.

To create a template:

1. Just create a normal virtual machine, install the OS, and the basic applications. Then remove the IP if manually assigned and shut down the VM. Right-click it, go to **Template** and then click **Convert to Template**, as in Figure 6-13.

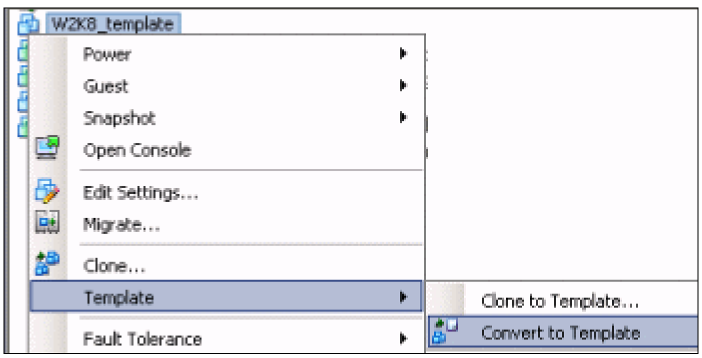



*Figure 6-13 Converting a VM to a template*

To see your template options, right-click one of your guests. Click **Inventory**. Select **Virtual Machines And Templates**., as in Figure 6-14, and you see a panel like this one.

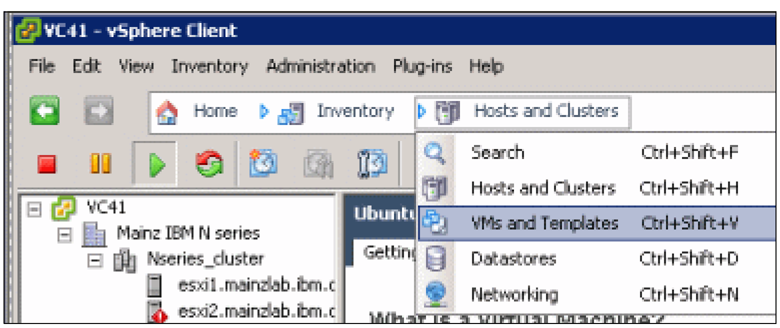



*Figure 6-14 Changing view to VMs and Templates*

You see all your templates as shown in Figure 6-15.

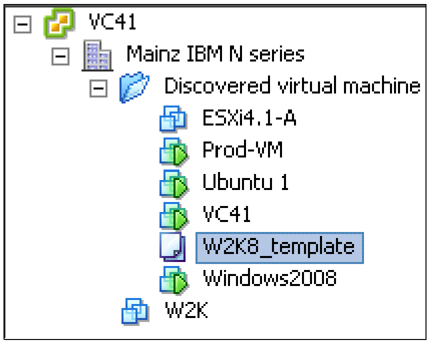



*Figure 6-15 Viewing VMs and Templates*

7

# Deploying LUNs on N series for VMware vSphere 4.1

This chapter explains how to set up the N series storage system for VMware ESX Server installation and for guest servers. It shows the boot options that are available for VMware ESX Servers. Finally, it guides you through the setup of logical unit numbers (LUNs) for installation of the guest servers.

This chapter includes the following topics:

- Preparing N series for the VMware ESXi Server
- Preparing N series LUNs for VMware vSphere
- Partition alignment
- Storage growth management

## 7.1 Preparing N series LUNs for VMware vSphere

When provisioning LUNs for access through FC or iSCSI, LUNs must be masked so that only the appropriate hosts can connect to them. Within Data ONTAP, LUN masking is handled by the creation of initiator groups (igroup).

An initiator group includes all of the FC worldwide port names (WWPNs) or iSCSI qualified names (IQNs) of each of the VMware ESXi servers. This task is done from a pre-determined scope, so when assigning a LUN to an igroup, all the hosts listed within can see the LUNs.

The igroup scope design depends on the virtual environment design as a whole. If you are dividing your VMWare servers into clusters that support different application tiers, for example, you need to create an igroup for each of those clusters. That way you ensure that all the hosts within that cluster have access to the same LUNs. And you avoid having the hosts from one cluster being able to see LUNs that are not relevant to them.

**igroups for FC and iSCSI protocols:** If a cluster of servers is to use both the FC and iSCSI protocols, create separate igroups for the FC and iSCSI LUNs.

To identify the WWPN or IQN of the servers, for each VMware ESXi Server in vCenter, select a server. Then click the **Configuration** tab and select one of the storage adapters to see the SAN Identifier column, as in Figure 7-1.

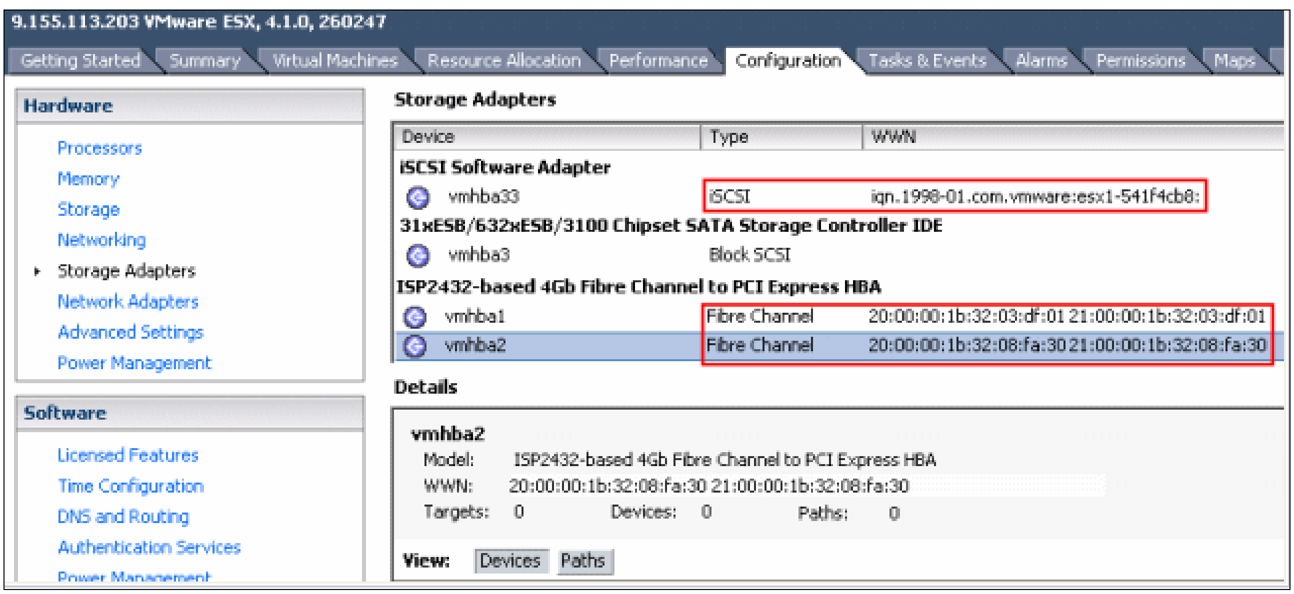


*Figure 7-1 Identifying WWPN or IQN numbers using the Virtual Infrastructure Client connected to vCenter*

The most common option for a VMware environment is to create LUNs and format them as VMFS (VMware file system) for the guest operating systems. The VMFS file system was developed by VMware and is used to store the guest operating system's disk files (.vmdk files) and its configuration files (.vmx files).

Other file extensions that are also part of the virtualization solution, such as Snapshot files, can also be stored in a VMFS volume. One of the main features of the VMFS file system is the ability to manage multiple access and support large files. Each LUN formatted as VMFS for a guest operating system's store is called a *datastore*.

Figure 7-2 shows an example of using a datastore through the vCenter console.

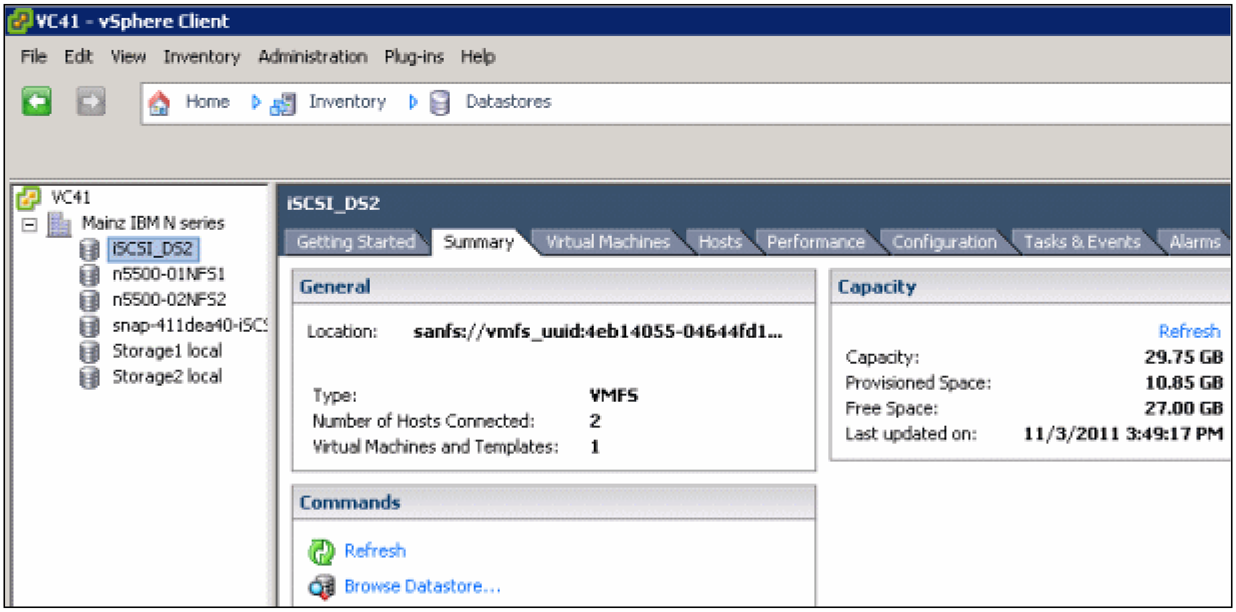



*Figure 7-2 A sample datastore*

## 7.2 Setting up thin provisioning

You can enable thin provisioning at the LUN level or volume level by using either the CLI or the GUI. The following sections guide you through this process using the GUI during the creation of the volumes or LUNs.

### 7.2.1 Enabling volume-level thin provisioning

To enable volume level thin provisioning, follow these steps:

1. In the left navigation pane of FilerView, select **Volumes** → **Add** (Figure 7-3).

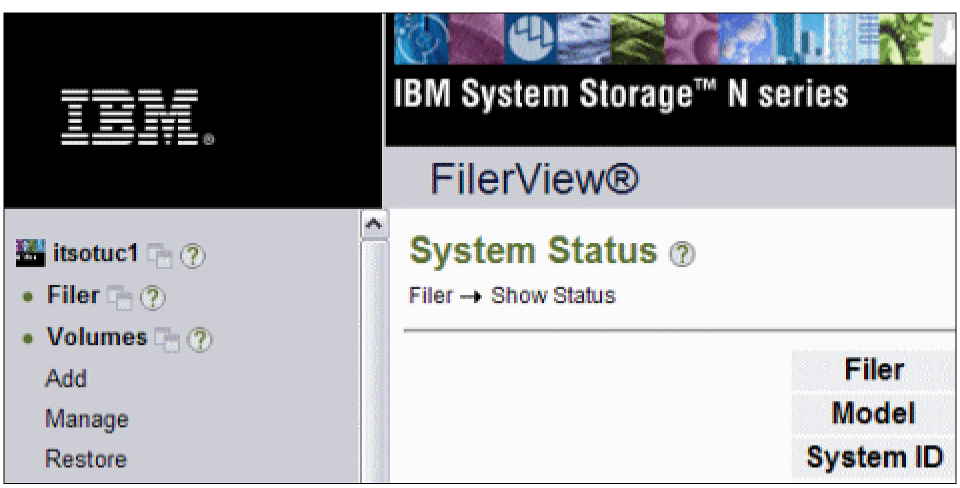



*Figure 7-3 Selecting the Add option*

2. In the Welcome panel of the Volume Wizard (Figure 7-4), click **Next**.

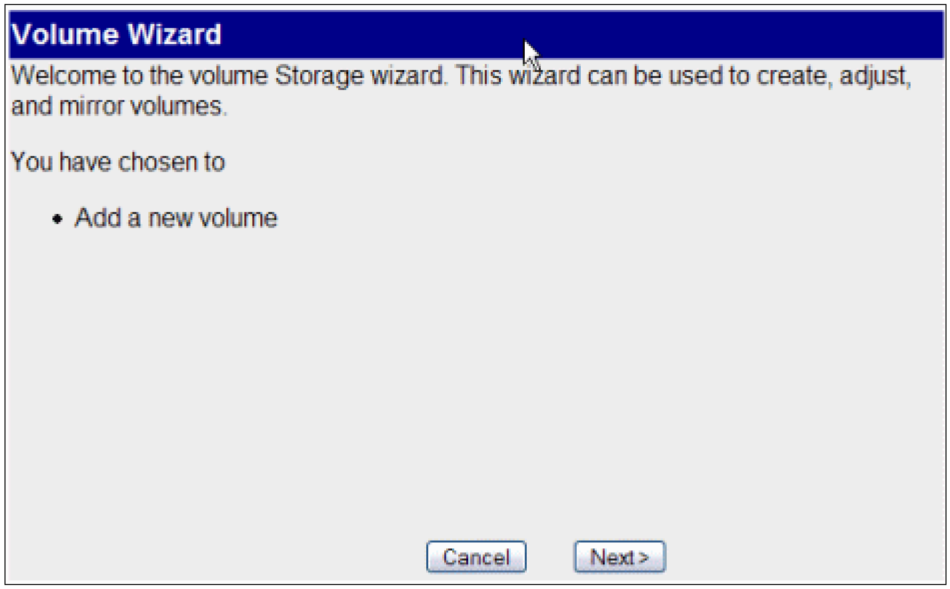



*Figure 7-4 Volume Wizard Welcome panel*

3. In the Volume Type Selection panel (Figure 7-5), select the type of volume you want to create. The Flexible option is the most popular because of its useful properties. Therefore, in this example, we select **Flexible**. Click **Next**.

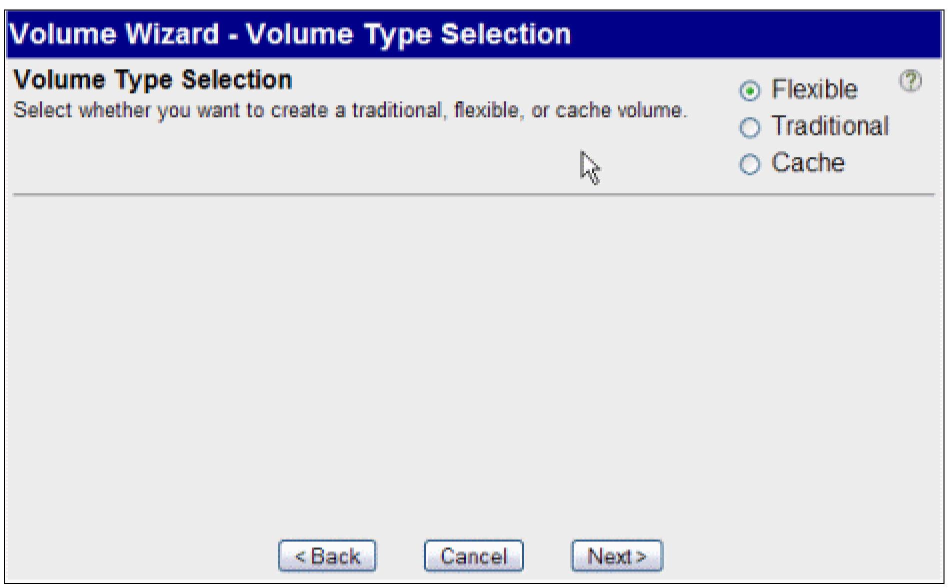



*Figure 7-5 Selecting the volume type*

4. In the Volume Parameters panel (Figure 7-6), enter a volume name of your choice. In this example, we choose *vol1* and accept the default settings of the other fields. Click **Next**.

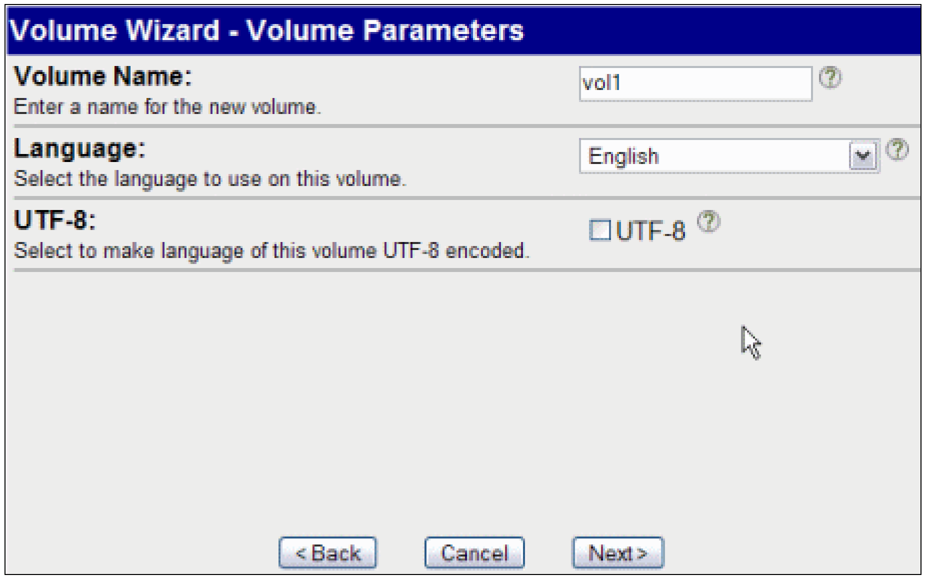



*Figure 7-6 Naming the volume parameters*

5. In the Flexible Volume Parameters panel (Figure 7-7), for Containing Aggregate, select the aggregate where you want to create the volume. For Space Guarantee, select **none**. This option enables volume-level thin provisioning. Then click **Next**.

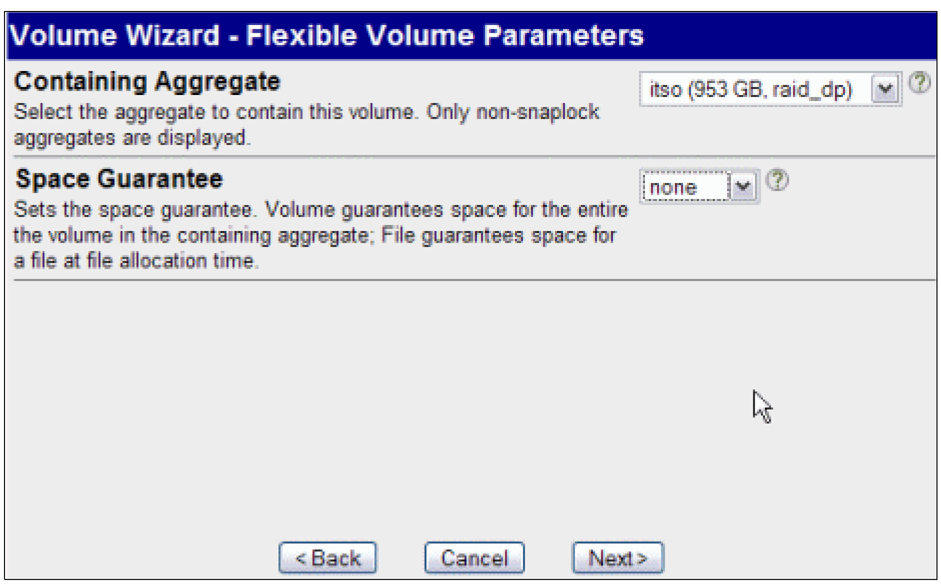



*Figure 7-7 Specifying the flexible volume parameters*

6. Select the size of the volume and the percentage reserved for snapshots, and click **Next**.
7. Click **Commit** to create the thin-provisioned volume.

8. Click **Close** to complete the process and close the Volume Wizard (Figure 7-8).

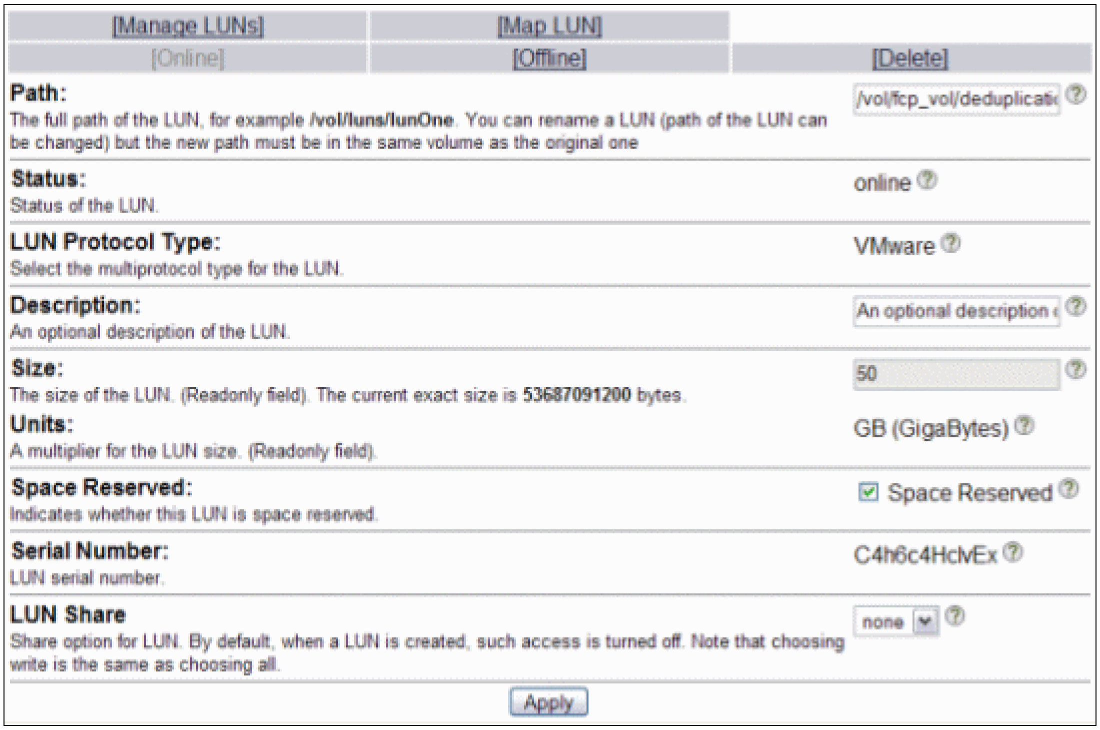


*Figure 7-8 Volume level thin provisioning*

## 7.2.2 Creating a thin provisioned LUN on N series systems

To create a thin provisioned LUN, follow these steps:

1. Open FilerView:

   `http://Nseries/na_admin`

2. Select **LUNs**.
3. Select **Wizard**.
4. In the Wizard window, click **Next**.
5. In the LUN Wizard: Specify LUN Parameters window (Figure 7-9), complete these steps:

   a. Enter the path.
   b. Enter the LUN size.
   c. Enter the LUN type. For VMFS, select **VMware**, or for RDM, select the guest OS type.
   d. Clear the **space-reserved** check box.
   e. Enter a description.
   f. Click **Next**.

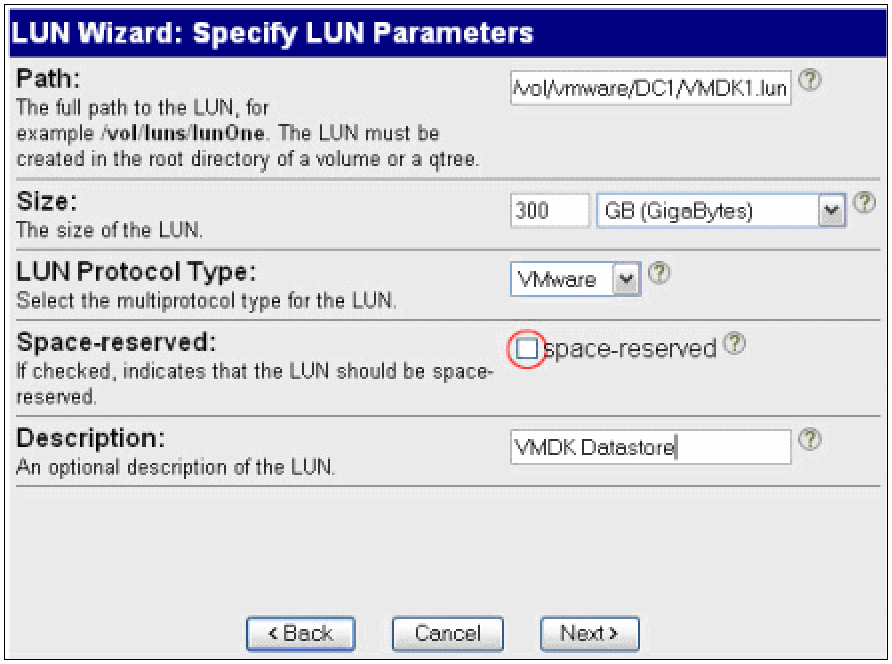



*Figure 7-9 Enabling thin provisioning on a LUN*

6. In the last window that opens, click **Finish**.

After the LUN is created, you see a message at the top of the window that says `LUN Create: succeeded`. You have now created a thin provisioned LUN. You can verify that it exists by running the command shown in Example 7-1.

*Example 7-1 LUN-level thin provisioning*

```
itsotuc3> df -g /vol/nfs_vol
Filesystem               total       used      avail capacity  Mounted on
/vol/nfs_vol/             50GB        2GB       47GB       5%  /vol/nfs_vol/
/vol/nfs_vol/.snapshot        0GB        0GB        0GB     ---%  /vol/nfs_vol/.
snapshot
itsotuc3>
```

When you enable N series thin provisioning, configure storage management policies on the volumes that contain the thin-provisioned LUNs. The use of these policies aids in providing the thin-provisioned LUNs with storage capacity as they require it. The policies include automatic sizing of a volume, automatic Snapshot deletion, and LUN fractional reserve.

*Volume Auto Size* is a policy-based space management feature in Data ONTAP. With this feature, a volume can grow in defined increments up to a predefined limit if the volume is nearly full. For VMware ESX Server environments, set this value to On, which requires setting the maximum volume and increment size options.

To enable these options, follow these steps:

1. Log in to the N series console.
2. Set the volume autosize policy with the following command:

```
vol autosize <vol-name> [-m <size> [k/m/g/t]] [-i <size> [k/m/g/t]] on
```

*Snapshot Auto Delete* is a policy-based space-management feature that automatically deletes the oldest Snapshot copies on a volume when that volume is nearly full. For VMware ESX Server environments, set this value to delete Snapshot copies at 5% of available space. In addition, set the volume option to have the system attempt to grow the volume before deleting Snapshot copies.

To enable these options, follow these steps:

1. Log in to the N series console.
2. Set the Snapshot autodelete policy with the following command:

```
snap autodelete <vol-name> commitment try trigger volume target_free_space 5
delete_order oldest_first
```

3. Set the volume autodelete policy with the following command:

```
vol options <vol-name> try_first volume_grow
```

*LUN Fractional Reserve* is a policy that is required when you use N series Snapshot copies on volumes that contain VMware ESX Server LUNs. This policy defines the amount of additional space reserved to guarantee LUN writes if a volume becomes 100% full. For VMware ESX Server environments where the following conditions exist, set this value to 0%.

- If Volume Auto Size and Snapshot Auto Delete are in use
- If you separated the temp, swap, pagefile, and other transient data onto other LUNs and volumes

Otherwise, leave this setting at its default of 100%.

To enable this option, follow these steps:

1. Log in to the N series console.
2. Set the volume Snapshot fractional reserve with the following command:

```
vol options <vol-name> fractional_reserve 0
```

### 7.2.3 Creating an initiator group on N series systems

To deliver a LUN to a server, set up the N series as follows:

1. Log in to the FilerView of your N series system, pointing a web browser to the IP of your storage.
2. In this example, we are setting up an initiator group for the iSCSI protocol:
   a. In the left pane of the FilerView panel, select **LUNs** → **LUN ConfigCheck** → **Initiator Groups**.
   b. In the Add Initiator Group panel (Figure 7-10), complete the following steps:
      i. For Group Name, choose any name you want for the initiator group. We use iSCSI_ig.
      ii. For Type, select the protocol that is to be used by the initiator group. In this case, select **iSCSI**.
      iii. For Operating System, select **VMware**, because the LUN is to be formatted as VMFS and is to be used by the guest operating systems.
      iv. For Initiators, enter the IQN of the ESX server.
      v. Click **Add**.

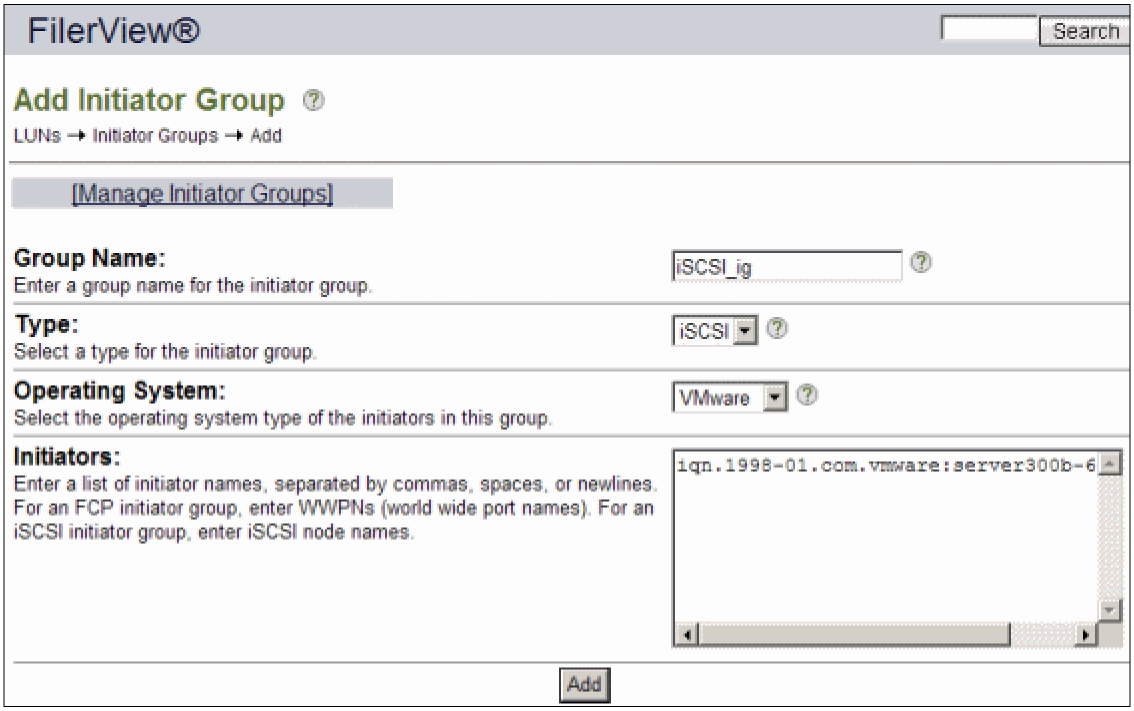



*Figure 7-10 Setting up the initiator group*

## 7.2.4 Creating a non-thin provisioned LUN on N series systems

1. Create a LUN for the initiator group iSCSI_ig. In the Add LUN pane (Figure 7-11), complete the following steps:
   a. For Path, give the path for the volume and the LUN name. In this example, we use the /vol/vol_vm_2/iSCSI path.
   b. For LUN Protocol Type, choose **VMware**.
   c. For Description, type any helpful description that you want.
   d. For Size, insert the size of the LUN.
   e. For Units, select the **GB (GigaBytes)** option because we are creating a 12-GB LUN.
   f. For Reserved Space, leave this check box selected so that the N series system can allocate all the space needed for this LUN.
   g. Click **Add**.

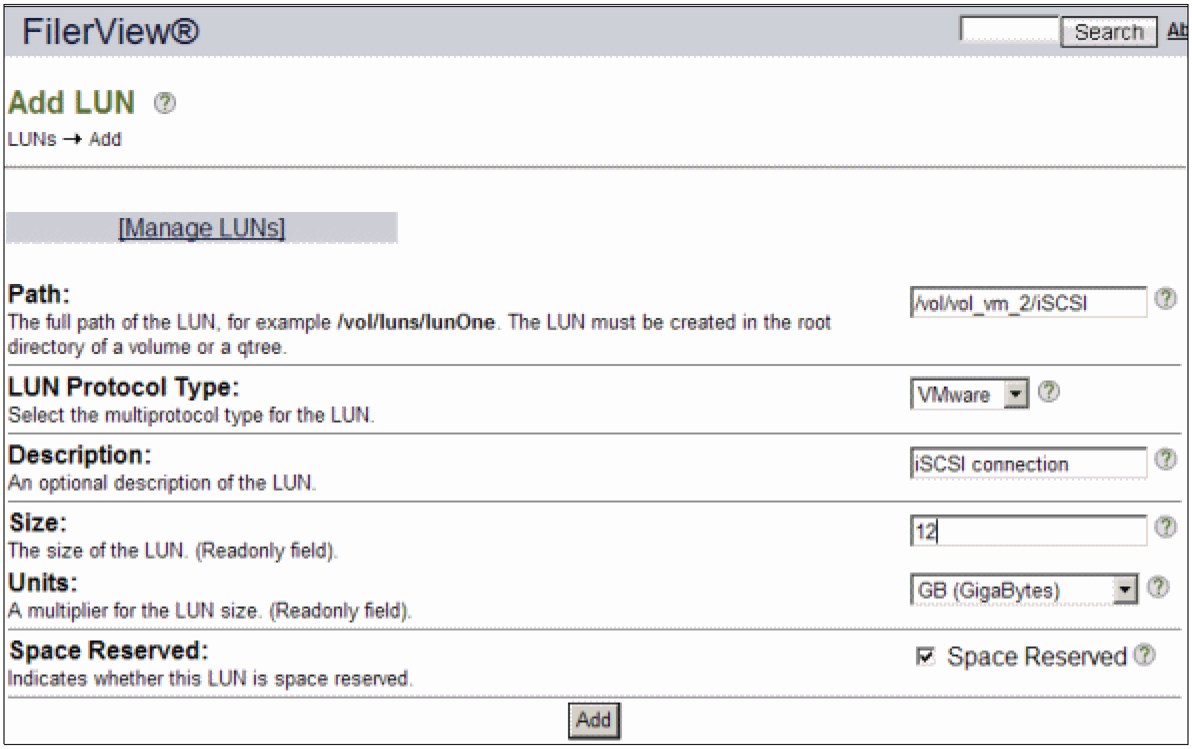
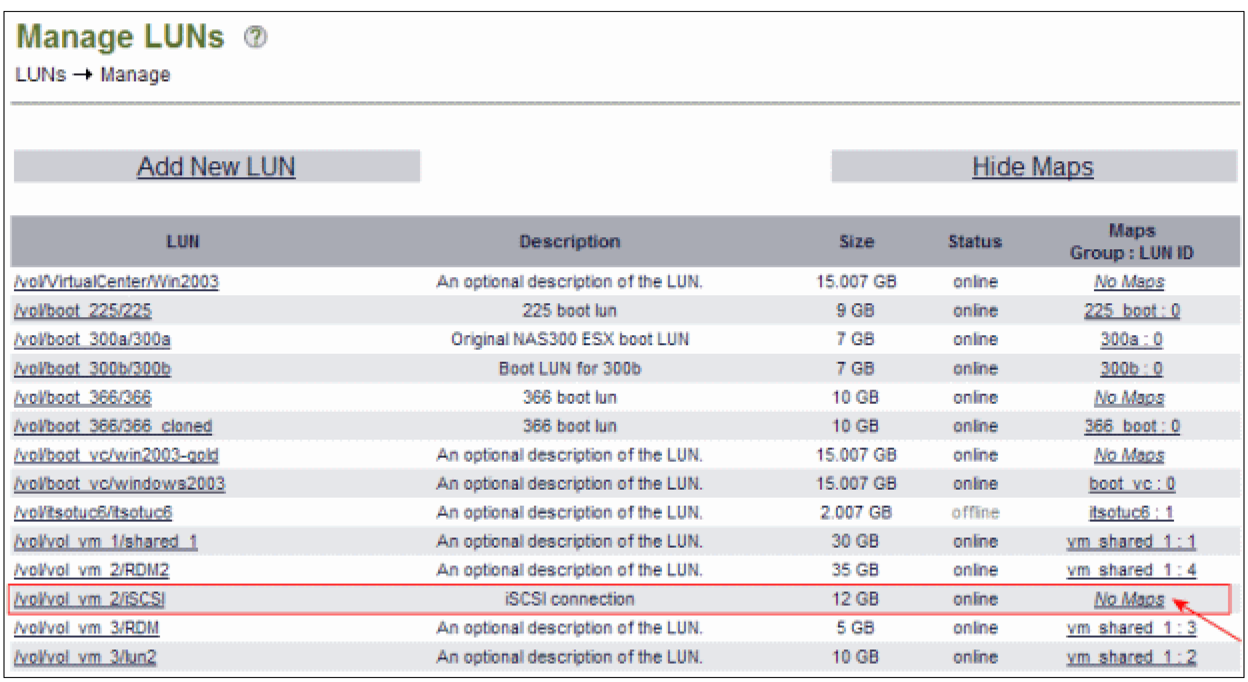



*Figure 7-11 Creating a LUN for the initiator group*

2. Map the new LUN to an initiator group (Figure 7-12):
   a. In the left pane of the FilerView panel, click **LUNs** → **Manage**.
   b. In the Manage LUNs pane, click the **No Maps** link.




| LUN | Description | Size | Status | Maps Group : LUN ID |
|---|---|---|---|---|
| /vol/VirtualCenter/Win2003 | An optional description of the LUN. | 15.007 GB | online | No Maps |
| /vol/boot_225/225 | 225 boot lun | 9 GB | online | 225_boot : 0 |
| /vol/boot_300a/300a | Original NAS300 ESX boot LUN | 7 GB | online | 300a : 0 |
| /vol/boot_300b/300b | Boot LUN for 300b | 7 GB | online | 300b : 0 |
| /vol/boot_366/366 | 366 boot lun | 10 GB | online | No Maps |
| /vol/boot_366/366_cloned | 366 boot lun | 10 GB | online | 366_boot : 0 |
| /vol/boot_vc/win2003-gold | An optional description of the LUN. | 15.007 GB | online | No Maps |
| /vol/boot_vc/windows2003 | An optional description of the LUN. | 15.007 GB | online | boot_vc : 0 |
| /vol/itsotuc6/itsotuc6 | An optional description of the LUN. | 2.007 GB | offline | itsotuc6 : 1 |
| /vol/vol_vm_1/shared_1 | An optional description of the LUN. | 30 GB | online | vm_shared_1 : 1 |
| /vol/vol_vm_2/RDM2 | An optional description of the LUN. | 35 GB | online | vm_shared_1 : 4 |
| /vol/vol_vm_2/iSCSI | iSCSI connection | 12 GB | online | No Maps |
| /vol/vol_vm_3/RDM | An optional description of the LUN. | 5 GB | online | vm_shared_1 : 3 |
| /vol/vol_vm_3/lun2 | An optional description of the LUN. | 10 GB | online | vm_shared_1 : 2 |

*Figure 7-12 Mapping the LUN to an initiator group*

c. In the LUN Map pane Figure 7-13, click **Add Groups to Map**.

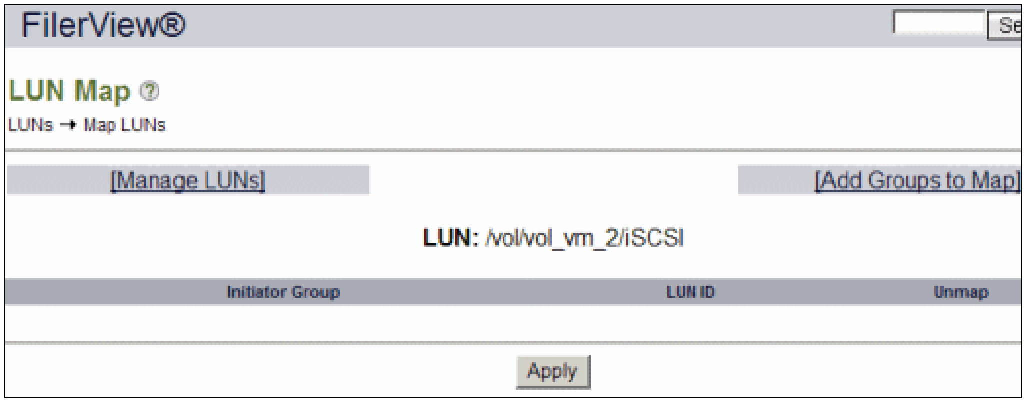



*Figure 7-13 Clicking the Add Groups to Map link*

d. In the LUN Map Add Groups pane (Figure 7-14), select the initiator group **iSCSI_ig** that we just created. Click **Add**.

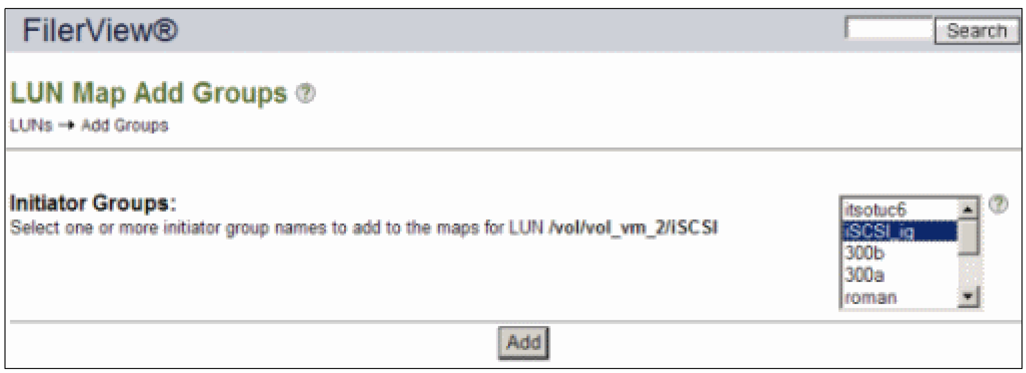



*Figure 7-14 Selecting the initiator group*

e. To complete the process, in the LUN Map pane (Figure 7-15), type the number that you want to assign to that LUN. Click **Apply**.

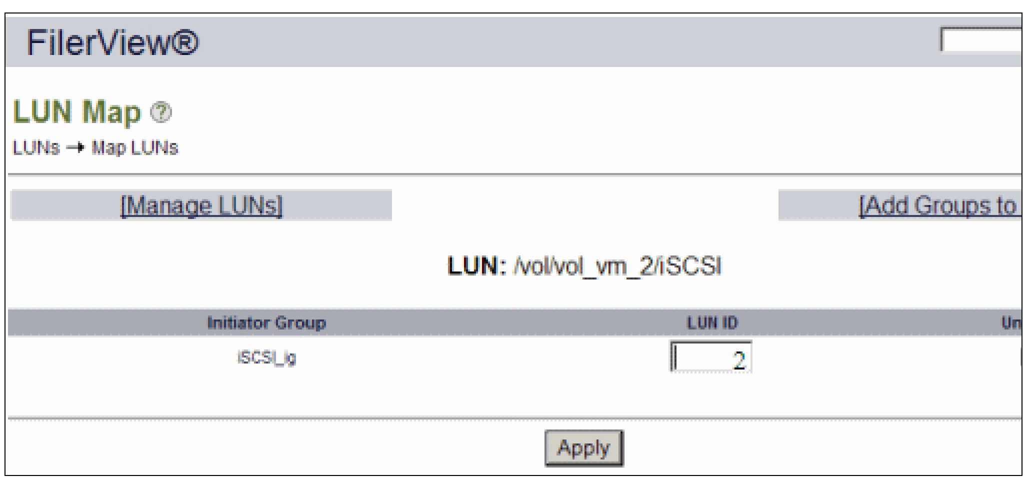
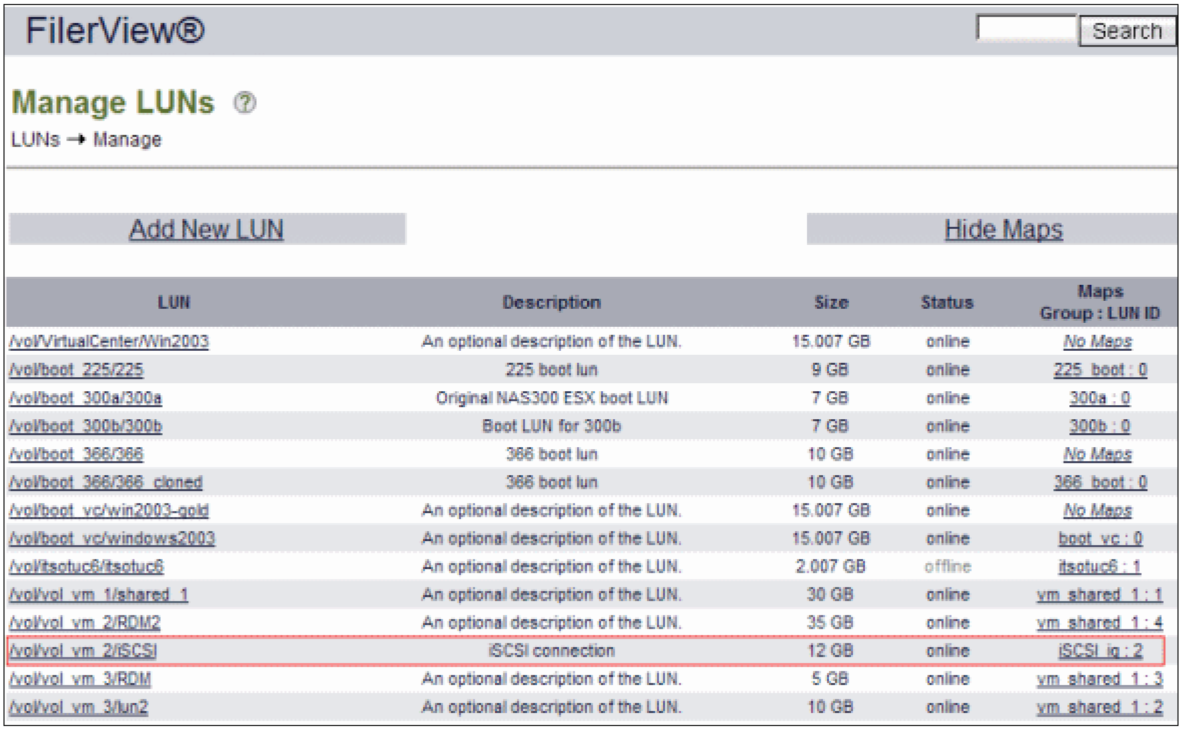



*Figure 7-15 Completing the mapping process*

The new LUN is now ready to be rescanned in vClient (Figure 7-16).




| LUN | Description | Size | Status | Maps Group : LUN ID |
|---|---|---|---|---|
| /vol/VirtualCenter/Win2003 | An optional description of the LUN. | 15.007 GB | online | No Maps |
| /vol/boot_225/225 | 225 boot lun | 9 GB | online | 225_boot : 0 |
| /vol/boot_300a/300a | Original NAS300 ESX boot LUN | 7 GB | online | 300a : 0 |
| /vol/boot_300b/300b | Boot LUN for 300b | 7 GB | online | 300b : 0 |
| /vol/boot_366/366 | 366 boot lun | 10 GB | online | No Maps |
| /vol/boot_366/366_cloned | 366 boot lun | 10 GB | online | 366_boot : 0 |
| /vol/boot_vc/win2003-gold | An optional description of the LUN. | 15.007 GB | online | No Maps |
| /vol/boot_vc/windows2003 | An optional description of the LUN. | 15.007 GB | online | boot_vc : 0 |
| /vol/itsotuc6/itsotuc6 | An optional description of the LUN. | 2.007 GB | offline | itsotuc6 : 1 |
| /vol/vol_vm_1/shared_1 | An optional description of the LUN. | 30 GB | online | vm_shared_1 : 1 |
| /vol/vol_vm_2/RDM2 | An optional description of the LUN. | 35 GB | online | vm_shared_1 : 4 |
| /vol/vol_vm_2/iSCSI | iSCSI connection | 12 GB | online | iSCSI_ig : 2 |
| /vol/vol_vm_3/RDM | An optional description of the LUN. | 5 GB | online | vm_shared_1 : 3 |
| /vol/vol_vm_3/lun2 | An optional description of the LUN. | 10 GB | online | vm_shared_1 : 2 |

*Figure 7-16 iSCSI - LUN ready for use*

## 7.2.5 Adding licenses to N series systems

Before you create a LUN in the N series system, you must properly license the protocols that are to be used to present the LUN to the host system. The protocols that we use are FCP, iSCSI, and Network File System (NFS).

To properly license the N series system, open the command prompt. Run **telnet** to the system, and use the **license add** command, as shown in Figure 7-17.

```
C:\> telnet 9.11.218.238

Data ONTAP (itsotuc4.itso.tucson)
login: root
Password: *******

itsotuc4*> license add <license_key>
```

*Figure 7-17 Adding a license to N series using telnet*

Alternatively, you can use FilerView to add the licenses to the N series system. After logging in the GUI, select **Filer** → **Manage Licenses** in the left pane, as shown in Figure 7-18.

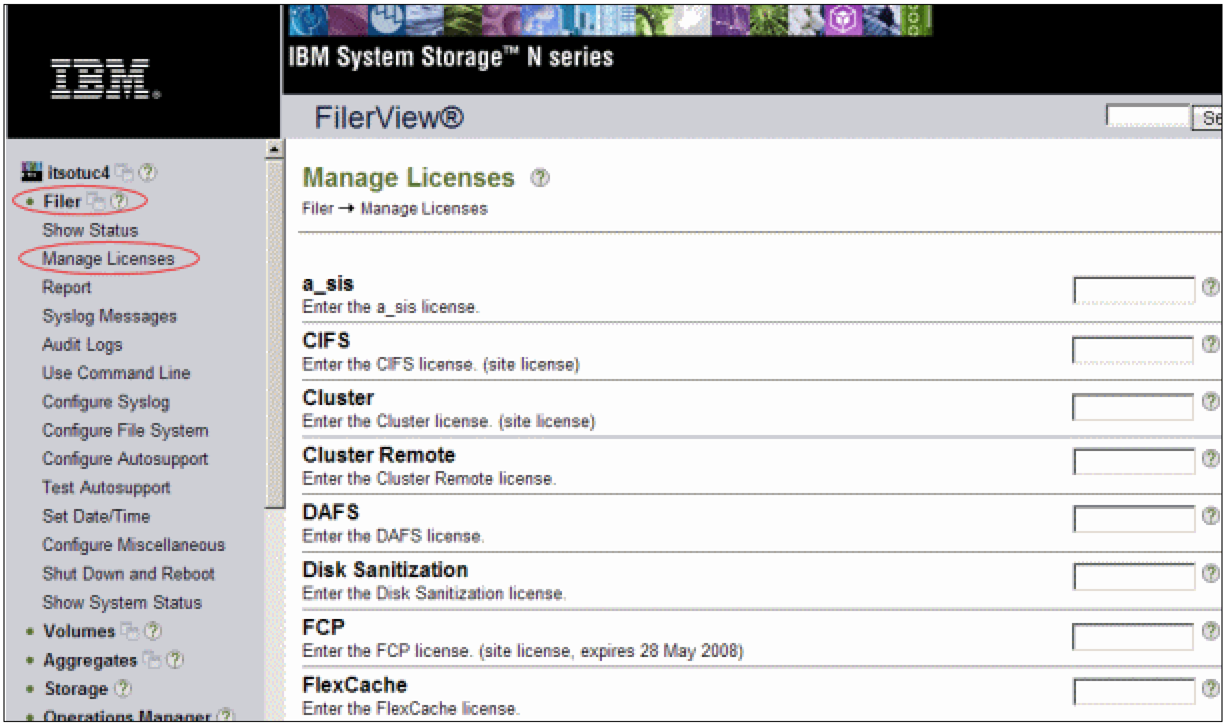


*Figure 7-18 FilerView to add licenses*

## 7.3 Presenting LUNs to an ESXi server over Fibre Channel

In this section, you allocate a LUN to a host, so it can be used as a datastore and provide virtual disks for your virtual machines.

The following steps are considered to be completed prerequisites before you proceed:

- Creation of a LUN
- An FCP Initiator Group with the WWPNs of the ESX hosts
- The mapping of that LUN to the FCP Initiator group

Follow these steps to create a VMFS datastore over an FC LUN:

1. Click the **Virtual Infrastructure Client** icon to launch the console.
2. Point to your vCenter IP or name, then enter your user name and password when prompted.
   - Use a domain account to log in if your vCenter server is part of a domain.
   - Otherwise, use a local account of the vCenter server, as shown in Figure 7-19.

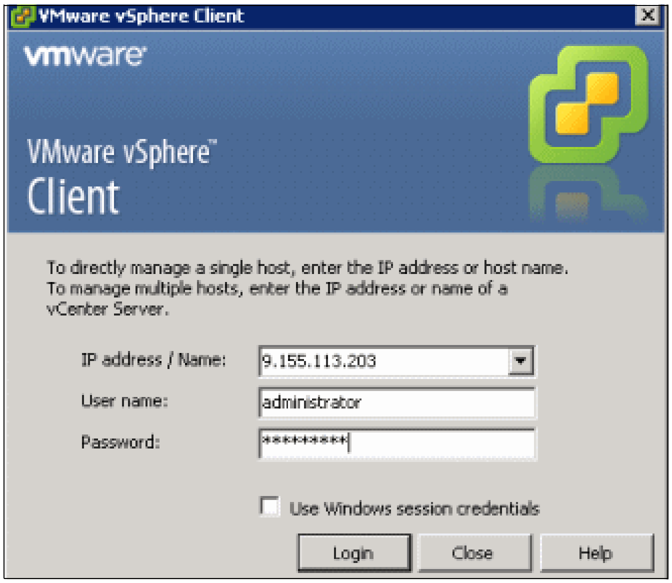



*Figure 7-19 Logging using the Virtual Infrastructure Client*

   After the console is opened, you can see the ESX host in the left pane and its properties in the right pane.

3. Rescan the storage LUNs to make the new LUNs available to the ESX host:
   a. Select the **ESXi Host**.
   b. On the **Configuration** tab, click **Storage**. Click the **Rescan** link.

   Selecting **Rescan** forces a rescan of all Fibre Channel and iSCSI HBAs, which is how VMware ESXi discovers changes in the storage available for use.

4. Repeat these steps for each host in the data center.

> **Double scan:** Some FCP HBAs require you to scan them twice to detect new LUNs. See VMware KB1798 at the following web address for further details:
>
> http://kb.vmware.com/kb/1798

After the LUNs are identified, you can provision them to the host as a datastore or assign them to a guest as an RDM.

To add a LUN as a datastore, follow these steps:

1. With vCenter opened, select a host.
2. In the right pane, select the **Configuration** tab.

3. In the Hardware box, select the **Storage** link and click **Add Storage**, as shown in Figure 7-20.

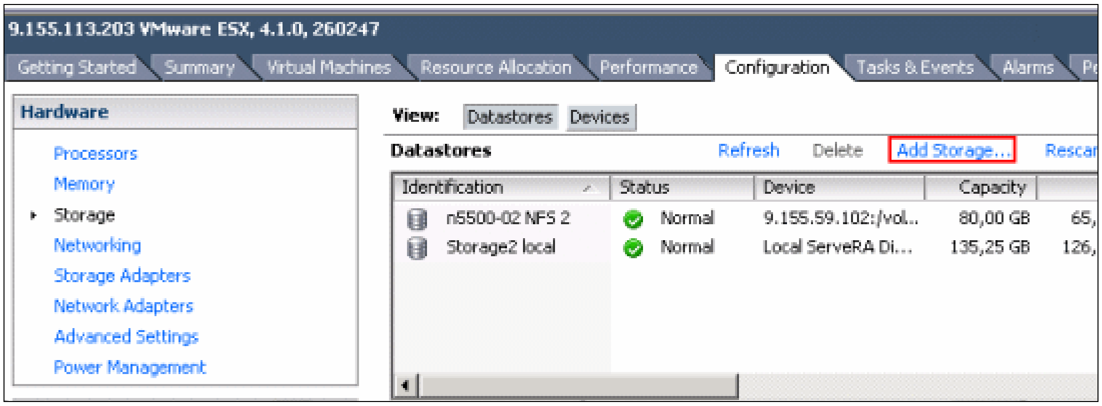



Figure 7-20 Adding storage

4. In the Add Storage wizard Figure 7-21, select the **Disk/LUN** radio button and click **Next**.

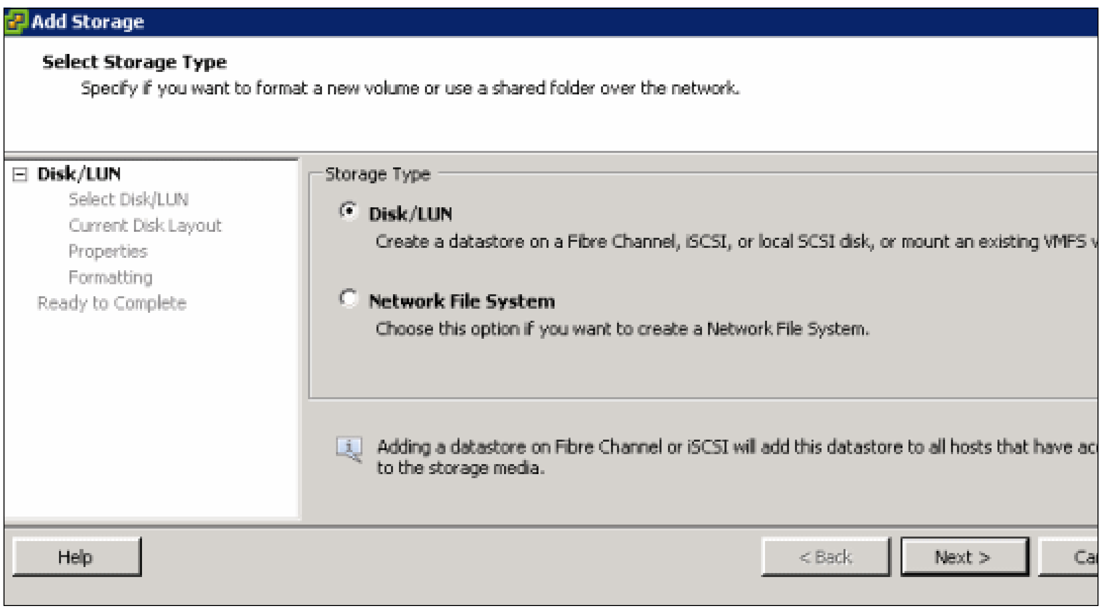



Figure 7-21 Add Storage wizard

5. Select the LUN that you want to use and click **Next** (Figure 7-22).

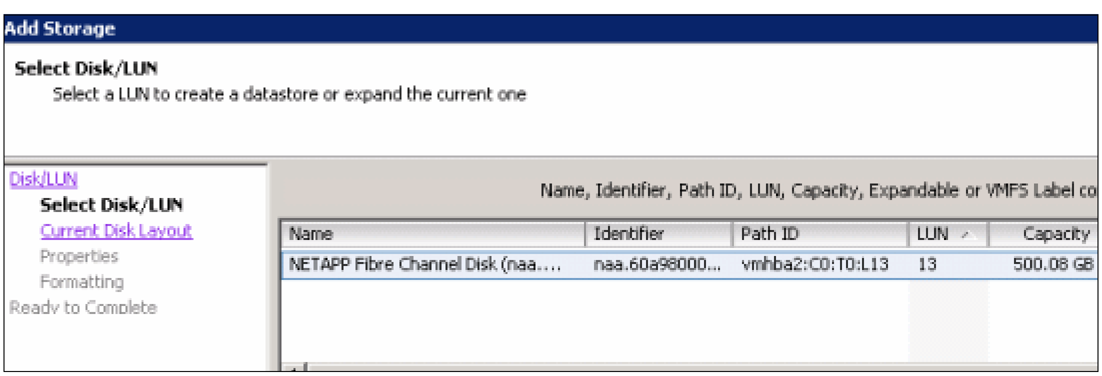



Figure 7-22 Selecting a LUN

6. Check the information about the LUN, which is shown to confirm that you selected the correct one, as in Figure 7-23. Determine if it is the desired LUN and click **Next.**

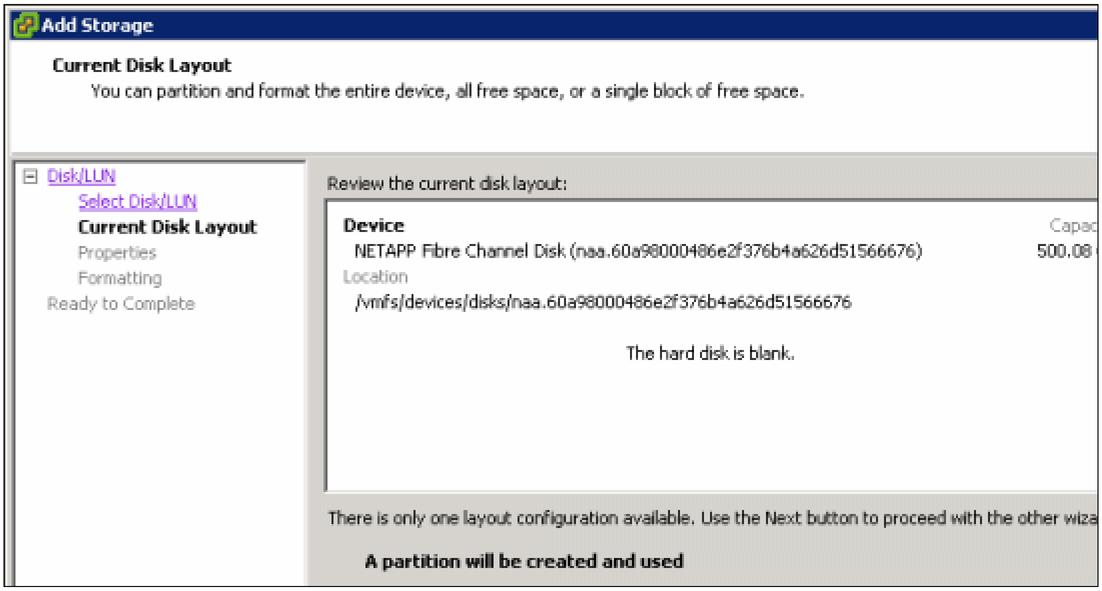



*Figure 7-23 LUN information*

7. Enter a name for the datastore and click **Next**.

   The default block size of datastores is 1 MB, which supports files up to a maximum of 256 GB in size. After you have formatted the datastore, there is no way to change the block size, unless you delete the datastore and recreate it with a different block size. For that reason, we advise using 8 MB, so you can have large files if you need them, as shown in Figure 7-24.

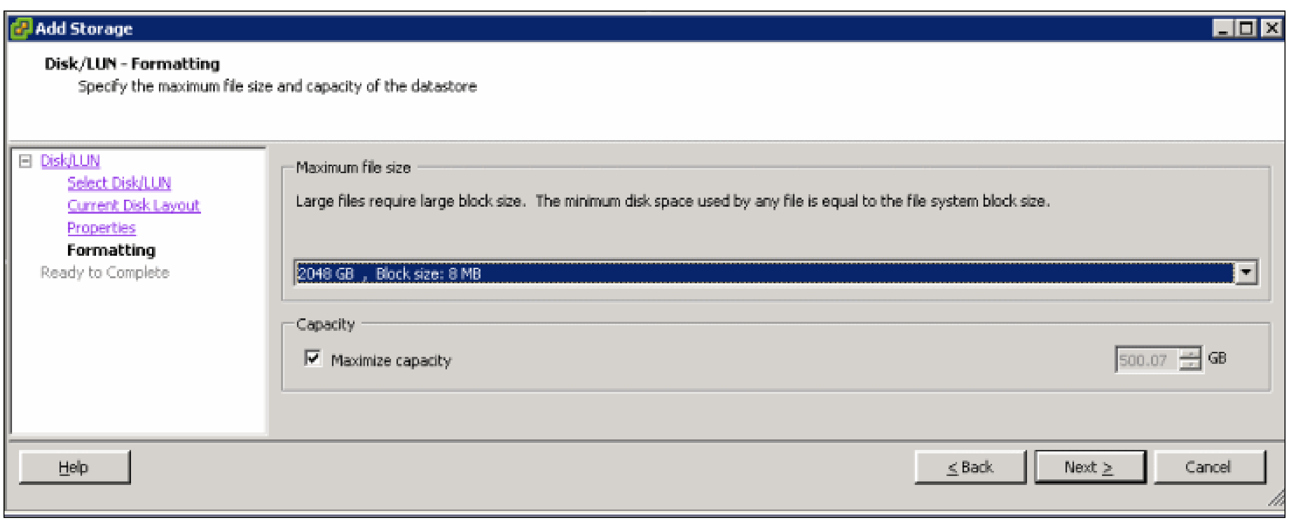



*Figure 7-24 VMFS block size*

8. Select the block size and click **Next**.

9. Review the information you typed and click **Finish** (Figure 7-25).

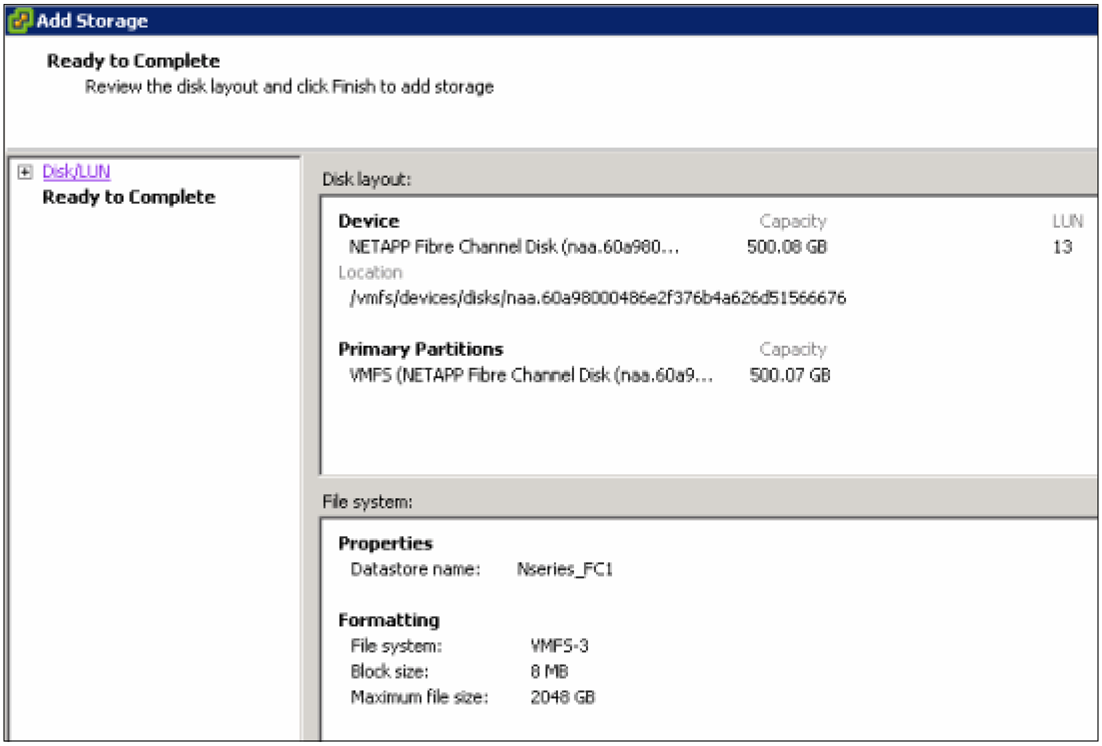



*Figure 7-25 Review the information before click finish*

10. Clicking the datastore, you can find the same information previously shown during the datastore creation (Figure 7-26).

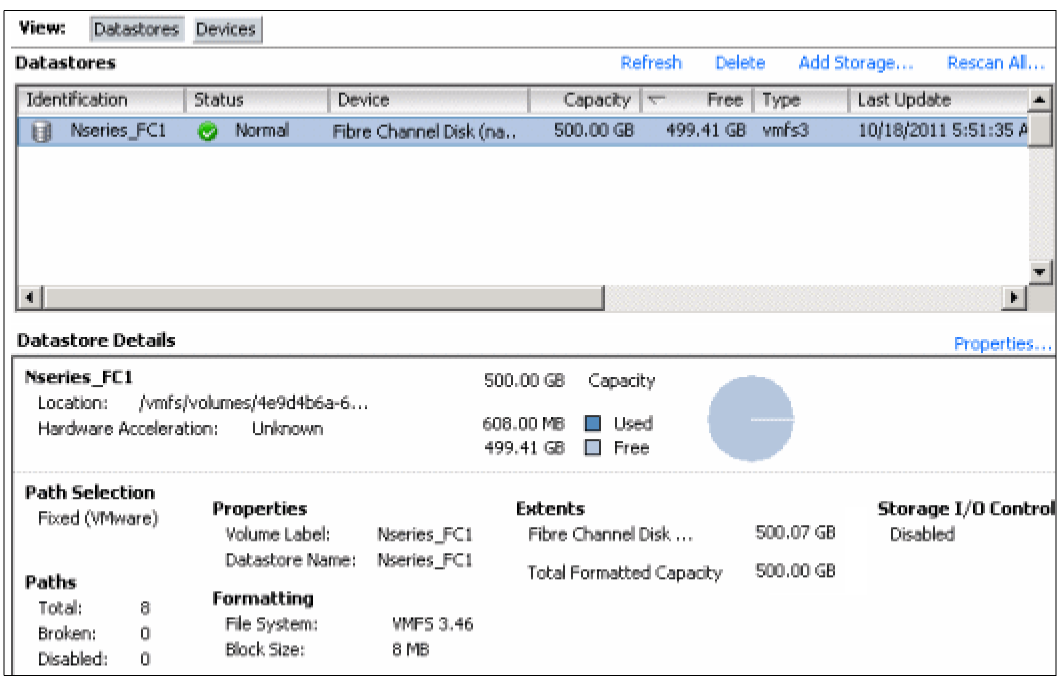



*Figure 7-26 Datastore information*

## 7.4 Using N series LUNs for Raw Device Mapping

With Raw Device Mapping (RDM), a guest operating system can access an external storage system regardless of the disk format. It is based on a VMDK file in a VMFS volume. This file is not a regular data file, but rather a pointer to external storage. This VMDK pointer file contains only the disk information describing the mapping to the external LUN of the ESX server.

RDM uses *dynamic name resolution* for access to the external storage system. With dynamic name resolution, you can give a permanent name to a device by referring to the name of the mapping file in the /vmfs subtree. All mapped LUNs are uniquely identified by VMFS, and the identification is stored in its internal data structures.

Any change in the SCSI path, such as a Fibre Channel switch failure or the addition of a new host bus adapter, has the potential to change the vmhba device name. The name includes the path designation (initiator, target, or LUN). Dynamic name resolution compensates for these changes by adjusting the data structures to re-target LUNs to their new device names.

The RDM device is most commonly used when virtual infrastructure administrators need to build a virtual-to-physical cluster where the quorum disk is mounted in an external storage device. You can only use RDM over the iSCSI protocol and FCP.

As an external storage system, RDM devices are compatible with such features as VMotion and snapshots (when in Virtual Compatibility mode). These devices are also fully visible and are configured through the Virtual Infrastructure Client console.

### 7.4.1 RDM compatibility mode

RDM devices can be used in virtual or physical mode:

- With virtual mode, you can use raw disks to realize the benefits of VMFS, such as advanced file locking for data protection and snapshots. No direct access is available to the external storage.
- In physical mode, the guest operating system has direct access to the raw physical storage with a minimum of virtualization layer. When using physical mode, you lose the ability to use Snapshot on this raw device.

### 7.4.2 Attaching an RDM disk device to a virtual machine

To attach a raw device to a guest operating system, follow these steps:

1. Create a LUN in the N series storage system, as discussed in 5.3.1, “Preparing N series LUNs for the ESXi boot from SAN” on page 64.

> **Bootable LUN:** The procedure described in 5.3.1, “Preparing N series LUNs for the ESXi boot from SAN” on page 64, refers to the creation of a bootable LUN. In this case, the LUN need not be bootable; it can be a regular LUN.

2. Go to the Virtual Infrastructure Client and rescan the datastore so that the ESX can reach the new LUN. On the **Configuration** tab, select the storage adapters, and then click **Rescan**.
3. Click the VM to which you want to add the RDM device, and click **Edit Settings**.
4. To add a new RDM device to the guest system, in the Virtual Machine Properties window (Figure 7-27), click the **Add** button.

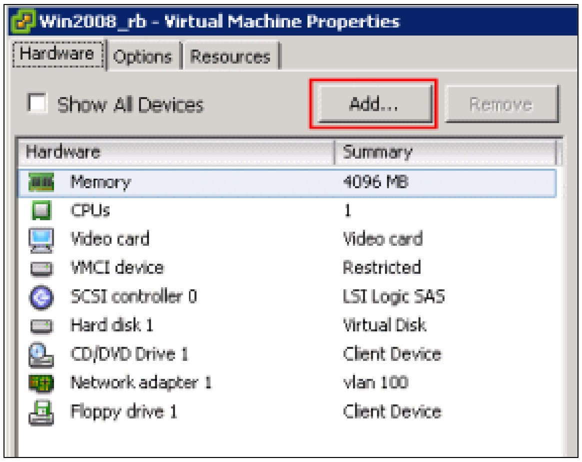



*Figure 7-27 Adding a new device*

5. In the Add Hardware Wizard – Select a Device Type panel (Figure 7-28), select **Hard Disk** and click **Next**.

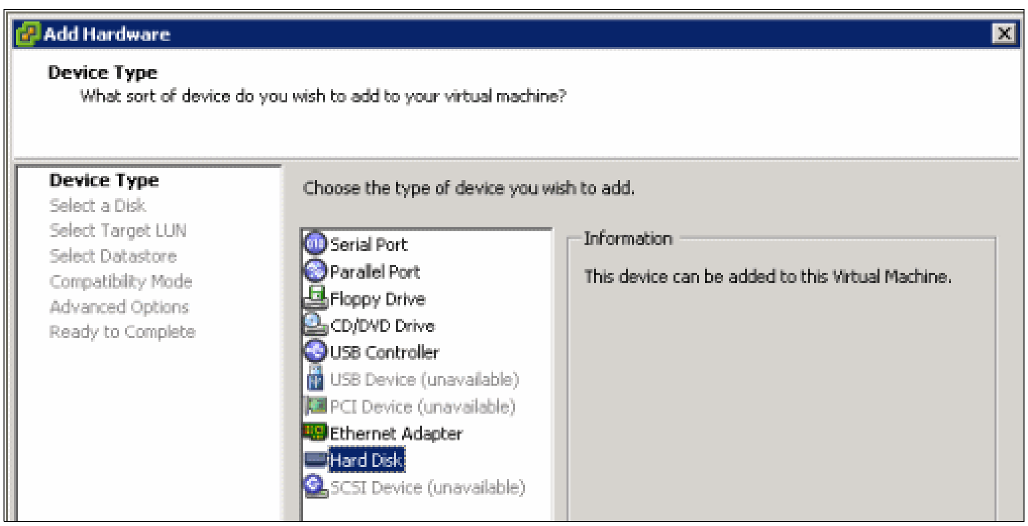



*Figure 7-28 Adding a new hard disk*

6. In the Select a Disk panel Figure 7-29, select **Raw Device Mappings**.

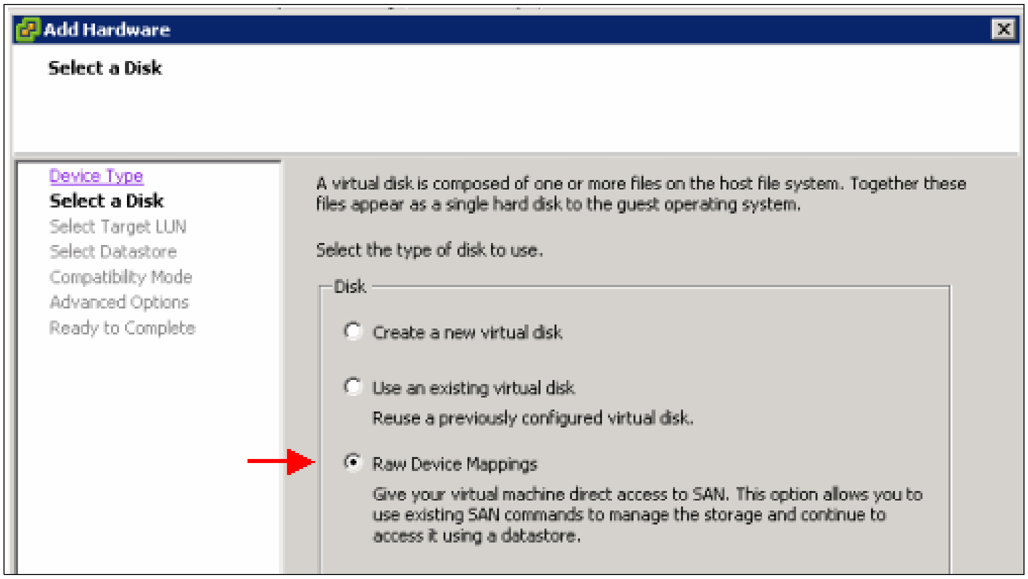



*Figure 7-29 Selecting the disk type*

7. In the Select and Configure a Raw LUN panel Figure 7-30, select the LUN that is to be mounted in this guest system. Then click **Next**.

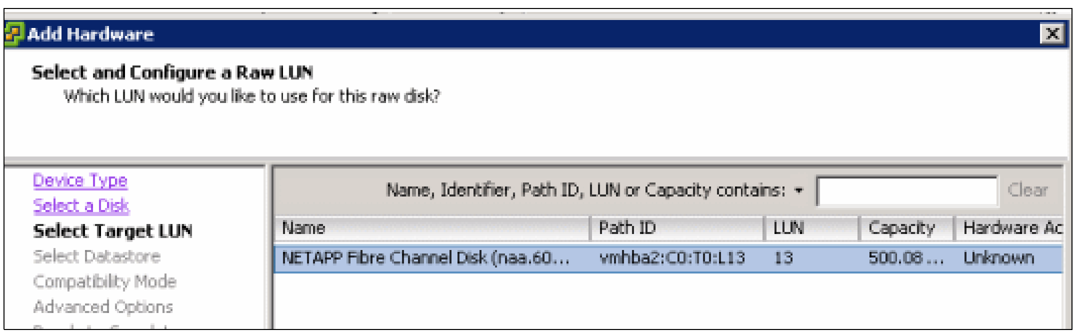



*Figure 7-30 Selecting the LUN*

8. In the Select a Datastore panel Figure 7-31, store the LUN mapping file either in the guest operating system directory or in another VMFS datastore. In this example, we choose the **Store with Virtual Machine** option. Then click **Next**.

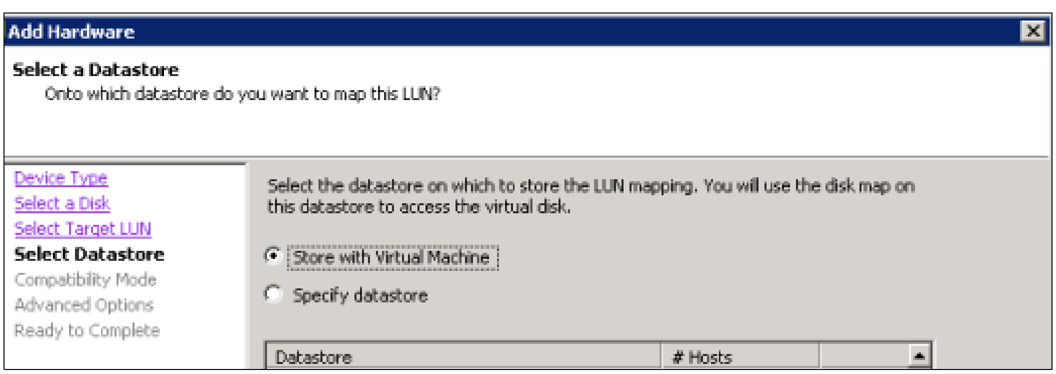



*Figure 7-31 Selecting the datastore to map the LUN*

9. In the Select Compatibility Mode panel (Figure 7-32), select **Physical**. For compatibility mode information, see 7.4.1, “RDM compatibility mode” on page 120. Click **Next**.

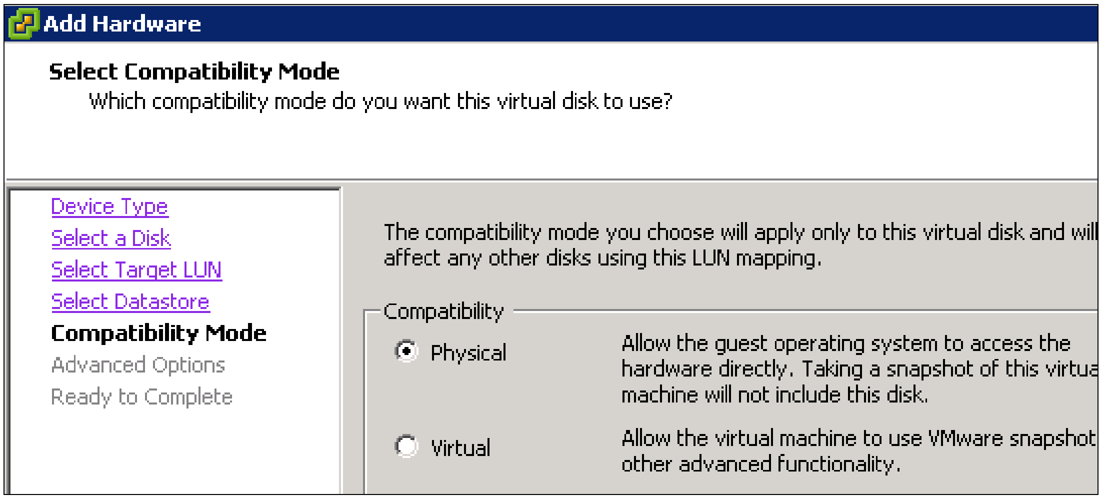



*Figure 7-32 Selecting the compatibility mode*

10. In the Specify Advanced Options panel (Figure 7-33), specify the virtual SCSI ID for the new disk device and for the SCSI mode. Accept the default options and click **Next**.

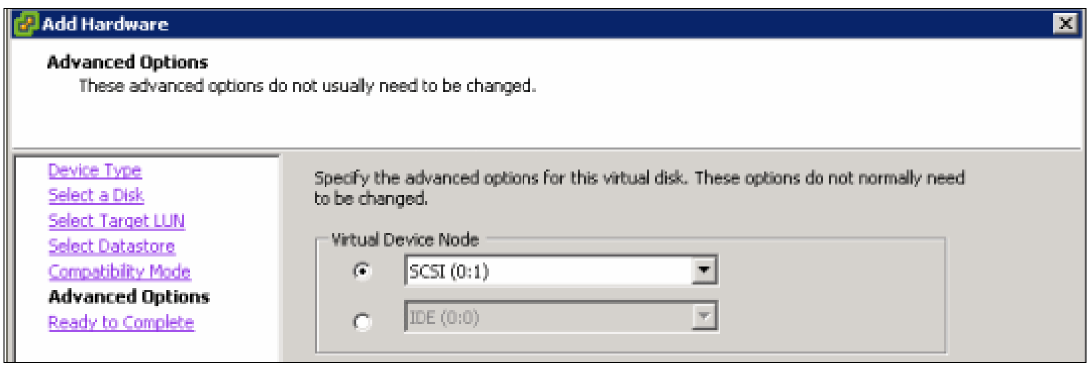



*Figure 7-33 Specifying the advanced options*

11. In the Ready to Complete panel (Figure 7-34), click **Finish** to confirm the settings.

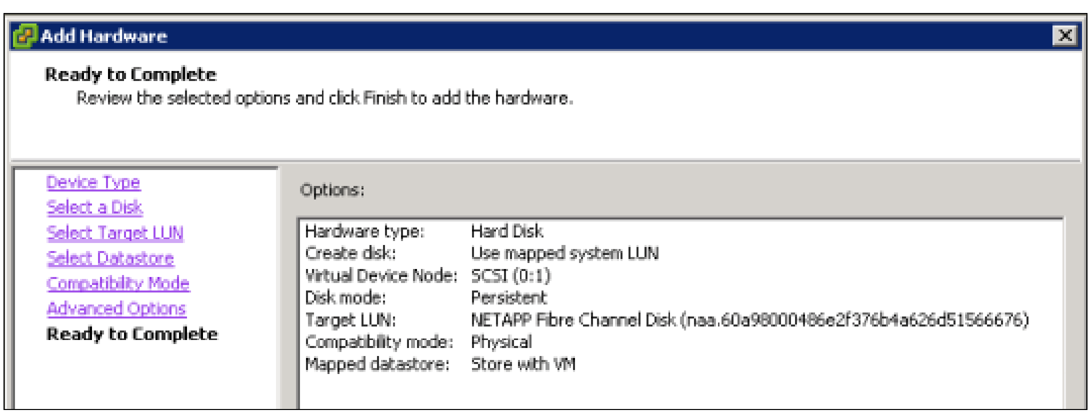



*Figure 7-34 Summary of settings*

12. After the wizard finishes, and you return to the Virtual Machine Properties window Figure 7-35, you see the new hard disk that you configured. Click **OK** to finish the process. When that is finished, the virtual machine is ready to use the RDM device.

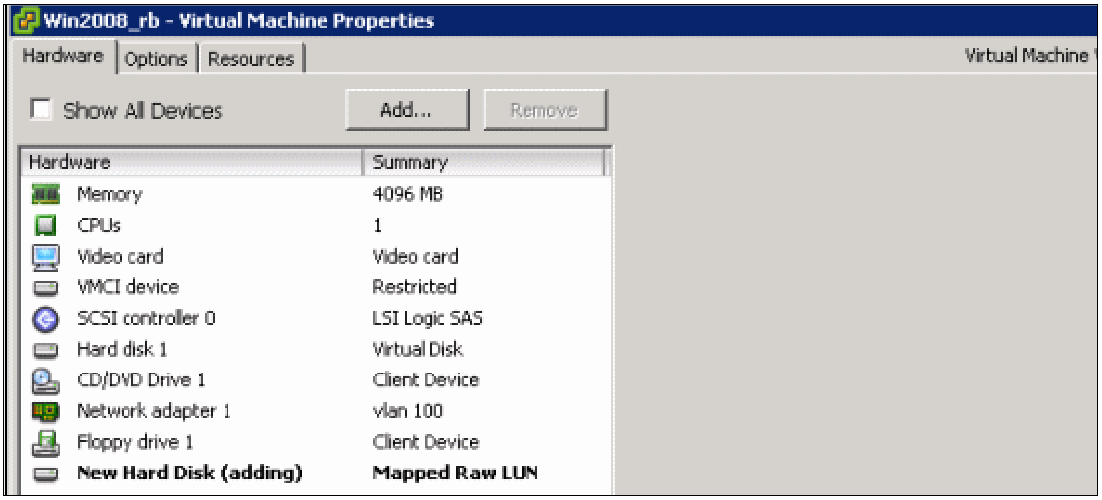



*Figure 7-35 RDM hard disk attached*

# 7.5 Creating a VMKernel portgroup on VMware vSphere 4.1

In order to communicate to a storage using the network (as opposed to accessing it through Fibre Channel), VMware requires a special connection named VMkernel.

VMkernel is a portgroup on a Virtual Switch (also known as vSwitch) that handles storage traffic and vMotion capacities. It is a best practice to separate the VMkernel used for vMotion from the one used for storage access. The purpose here is to ensure that each one does not affect the performance of the other one.

The following steps show how to set up a VMkernel portgroup, required for network storage access as iSCSI and NFS.

To configure the iSCSI connectivity, follow these steps:

1. Open vCenter.
2. Select a host.
3. In the right pane, select the **Configuration** tab.
4. In the Hardware box, select **Networking**.
5. In the upper right corner, click **Add Networking**, as in Figure 7-36.

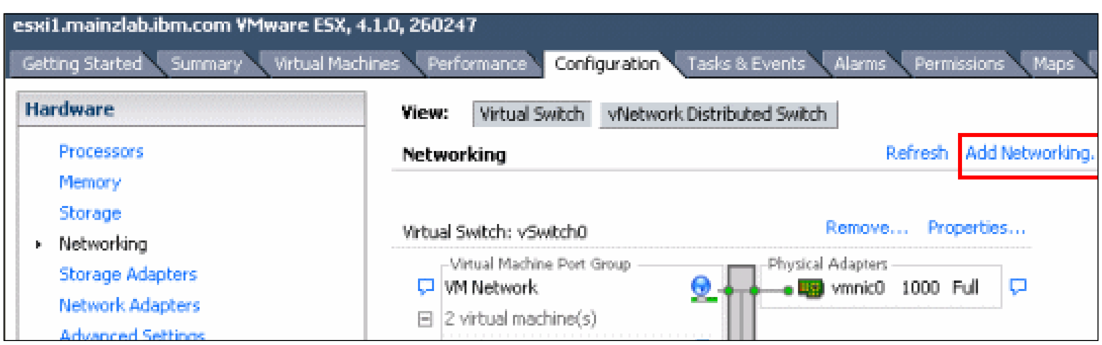



*Figure 7-36 Adding network*

6. In the Add Networking wizard (Figure 7-37), select the **VMkernel** radio button and click **Next**.

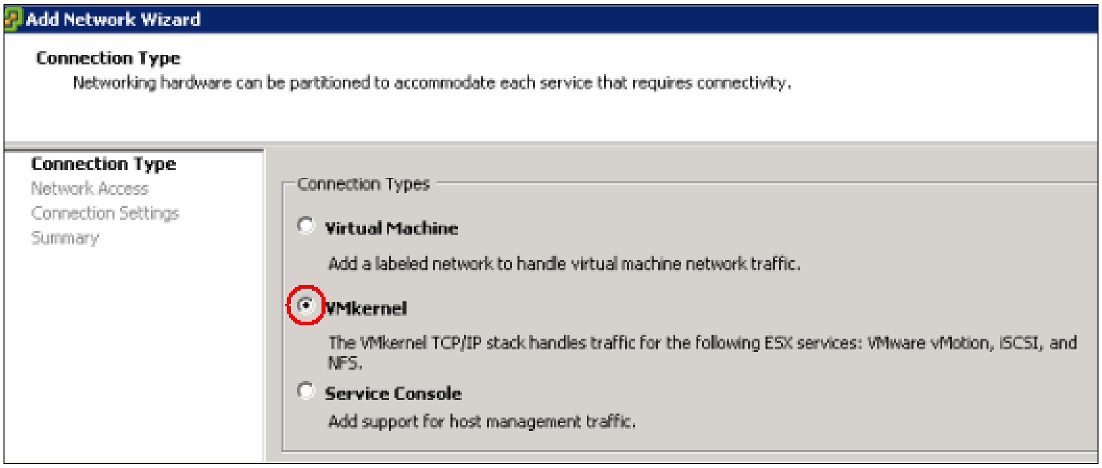



*Figure 7-37 Adding a VMkernel port*

7. Select the NIC that is to be bound to this switch, as shown in Figure 7-38.

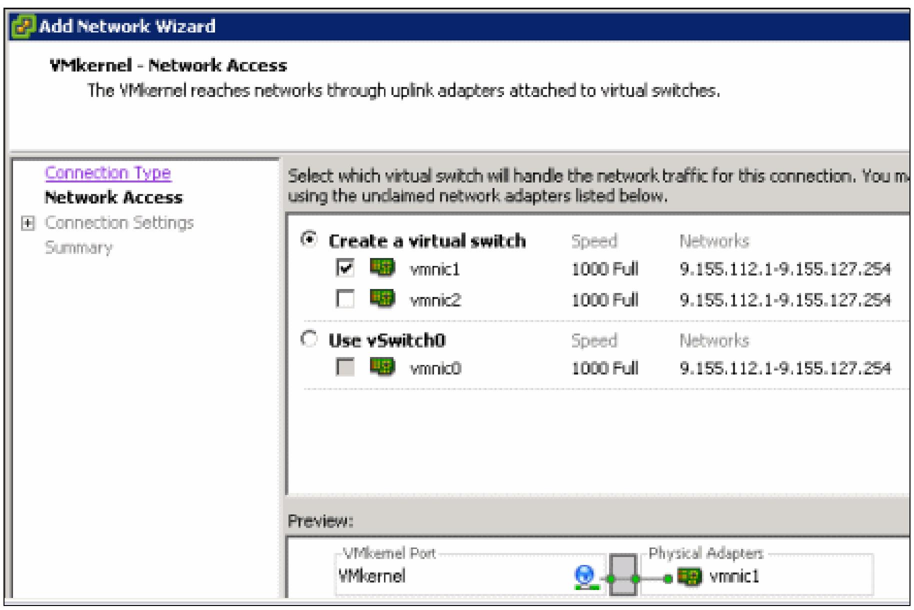



*Figure 7-38 Creating a new switch and selecting the physical NIC attached to it*

**Tip:** Although a vSwitch can have multiple NICs and portgroups, any given NIC can be bound to a single vSwitch only. That is why the vmnic0 is not available.

8. Enter a name for the portgroup that you are creating. A descriptive name can help to better identify the networks, thus easing management and troubleshooting. Because this portgroup is used to communicate with the storage only, none of the check boxes are marked. We named it VMKernel_storage, as in Figure 7-39.

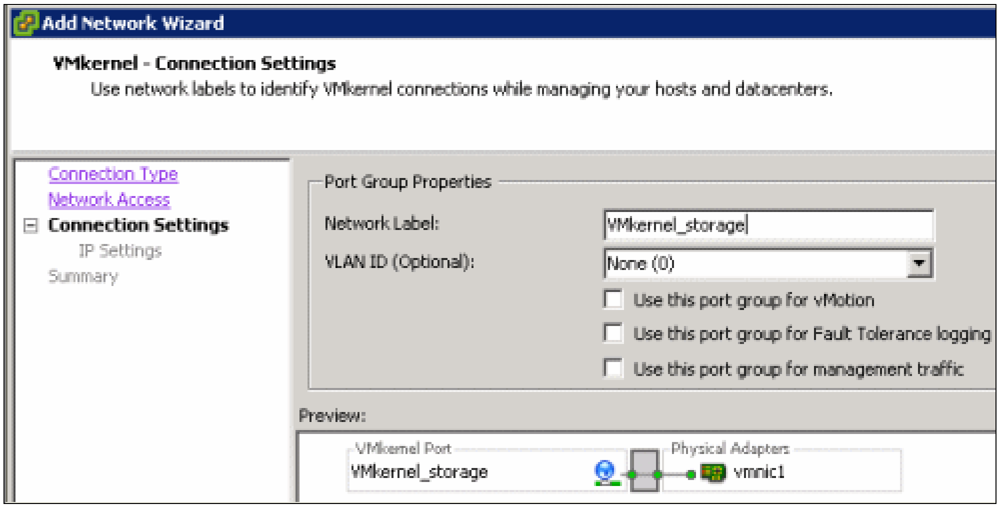



*Figure 7-39 Naming the portgroup*

9. Enter the IP information for the VMKernel portgroup, as in Figure 7-40, and then click **Next**. If you need to change your VMkernel Default Gateway, click **Edit** and change the address accordingly.

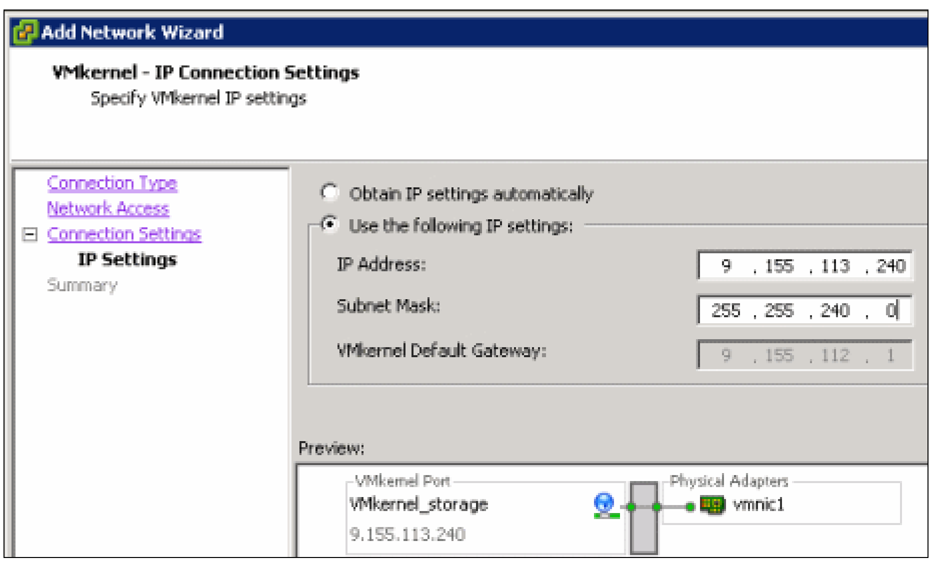



*Figure 7-40 IP configuration of VMKernel*

10. In the next panel, review the information entered and click **Finish** to create the VMKernel portgroup. Figure 7-41 shows the added vSwitch and its VMkernel portgroup.

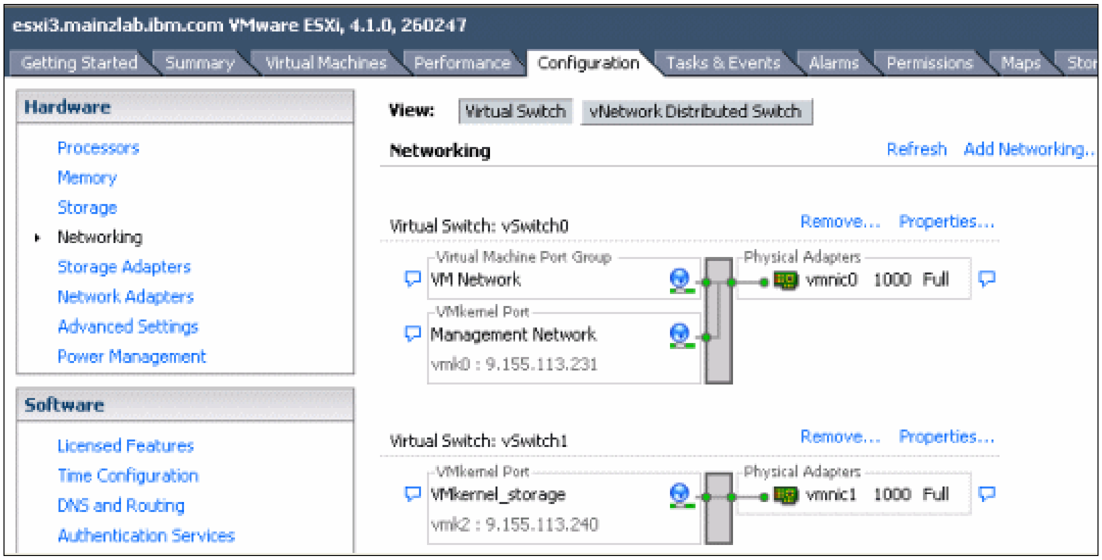



*Figure 7-41 The new vSwitch, named vSwitch1, and its VMkernel portgroup*

# 7.6 Presenting LUNs to VMware ESXi Server over iSCSI protocol

This section explains how to present a storage LUN to the VMware ESX host by using the iSCSI protocol:

1. Highlight the **iSCSI Adapter** and click the **Properties** link in the Details box, as shown in Figure 7-42.

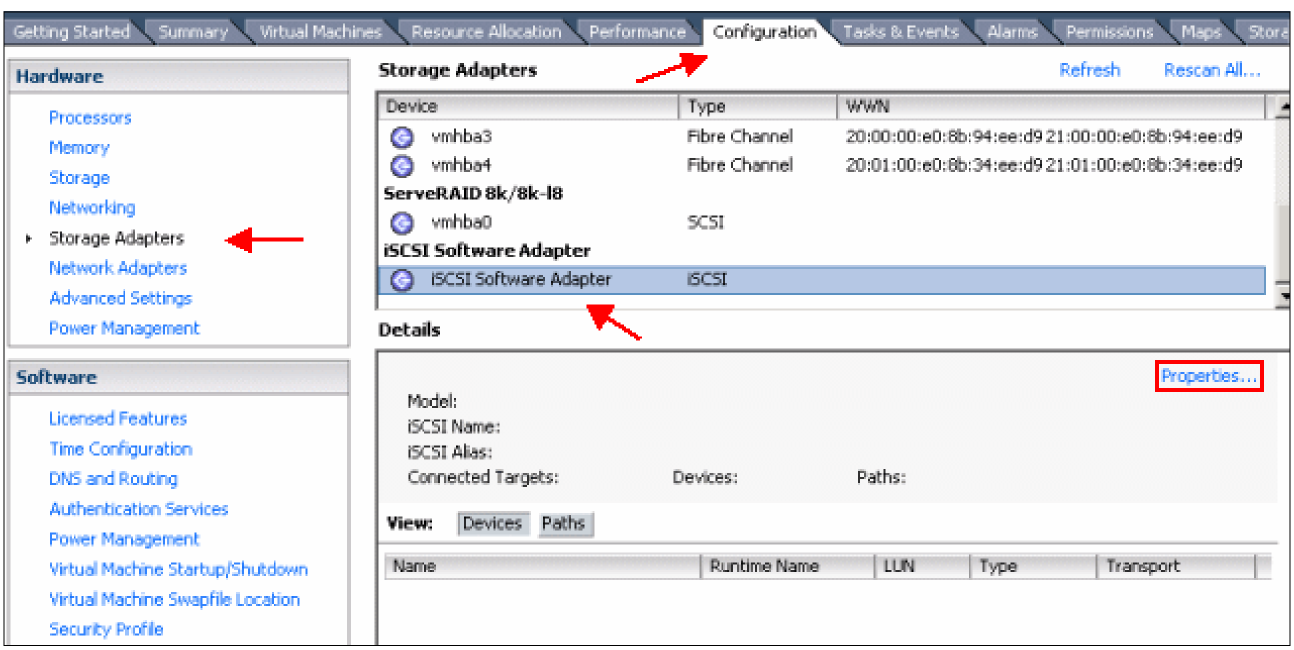



*Figure 7-42 Selecting an iSCSI initiator*

2. The iSCSI configuration panel displays. Click **Configure...** Then click the **Enable** select box, as shown in Figure 7-43.

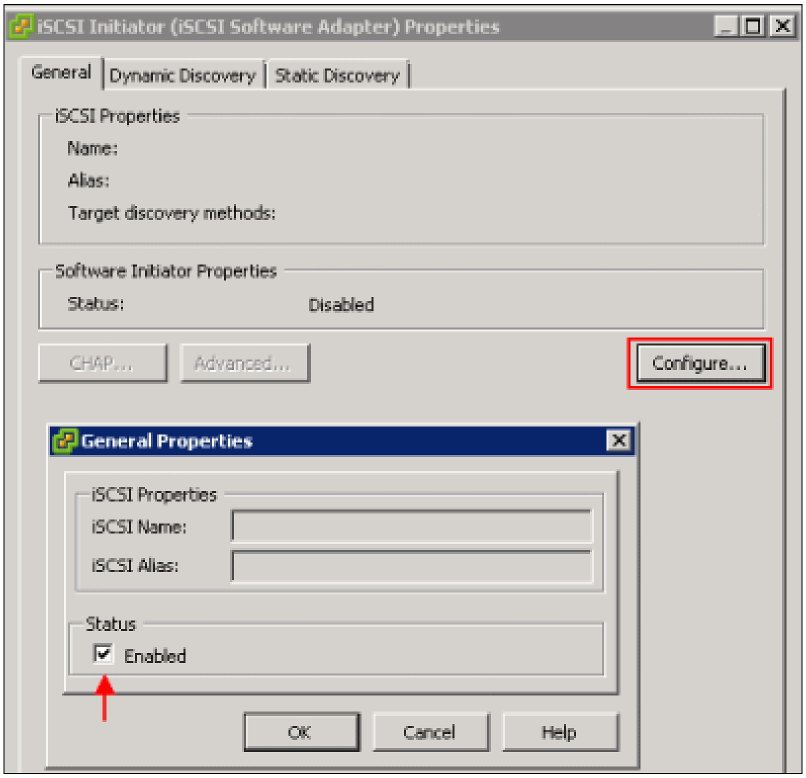



*Figure 7-43 Enabling iSCSI Software adapter*

3. The iSCSI software adapter is enabled, as shown Figure 7-44.

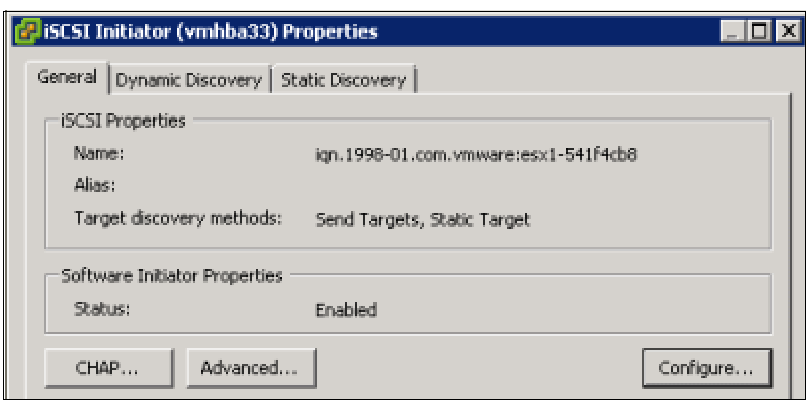



*Figure 7-44 An enabled iSCSI adapter, and its IQN*

4. In the iSCSI Initiator Properties window, select the **Dynamic Discovery** tab. Click **Add** and enter the IP address of the iSCSI-enabled interface of the N series system. Then type the IP address of the iSCSi target storage, then click **OK**.

5. Repeat these steps for all targets (Figure 7-45).

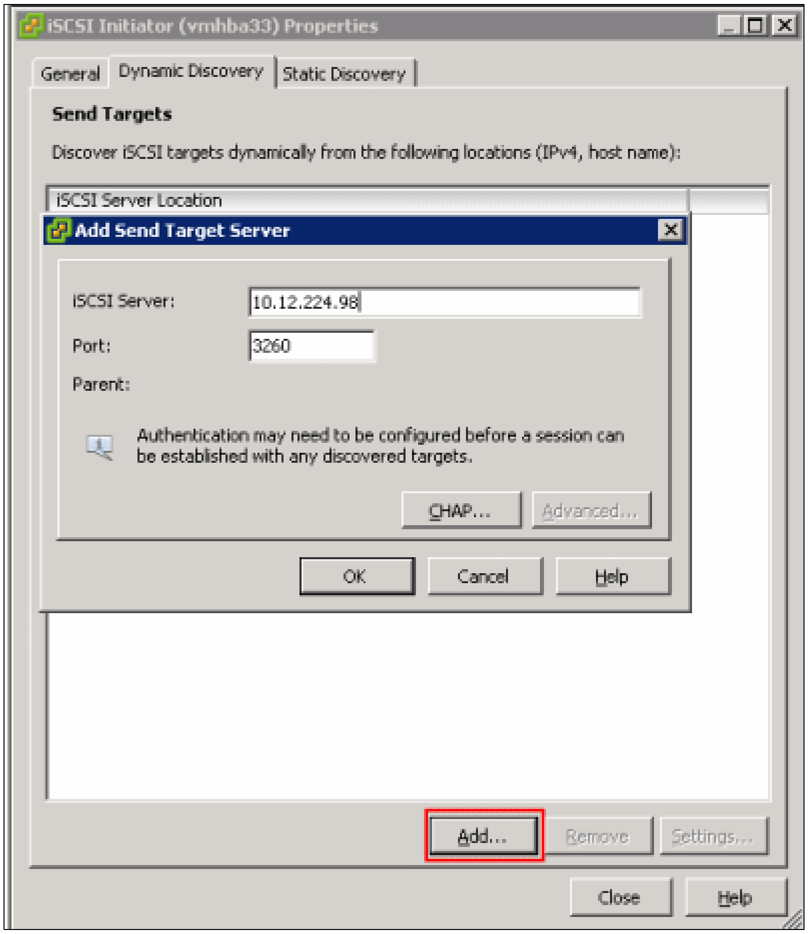



*Figure 7-45 Adding iSCSI targets*

6. For additional security, select the **CHAP Authentication** tab to configure CHAP Authentication. Verify iSCSI access before you enable CHAP Authentication.

## 7.7 Presenting an iSCSI LUN directly to a virtual machine

LUNs can be presented directly to virtual machines when using Fibre Channel through RDM. In the same way, LUNs can be directly accessed by a guest machine using iSCSI.

To implement this procedure, use the following steps:

1. On Windows 2008, click **Start** → **Administrative Tools** → **iSCSI Initiator**. On Windows 2003, the iSCSI client must be downloaded from the following website:

   `http://www.microsoft.com/download/en/details.aspx?id=18986`

   You can then install it by just accepting the defaults.

2. You might receive a message stating that the iSCSI service is not running yet. Click **Yes** to enable it.

3. On the iSCSI menu, click the **Configuration** tab and check the server's IQN, as shown in Figure 7-46. If you want to change it, click the **Change** button and make your modifications accordingly.

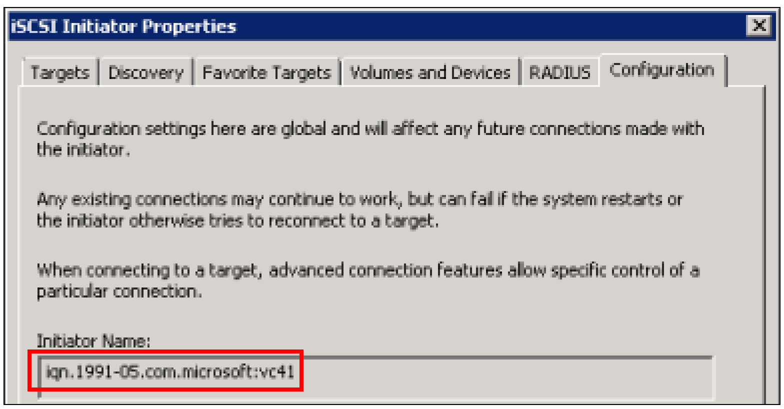



*Figure 7-46 Collecting the VM's IQN*

4. Create an iSCSI Initiator group, as described in 7.2.3, "Creating an initiator group on N series systems" on page 110.

5. Create and assign a LUN to it.

6. Click the **Discovery** tab, then click **Discover Portal**. Type the N series data IP interface for "IP address or DNS name", as shown in Figure 7-47.

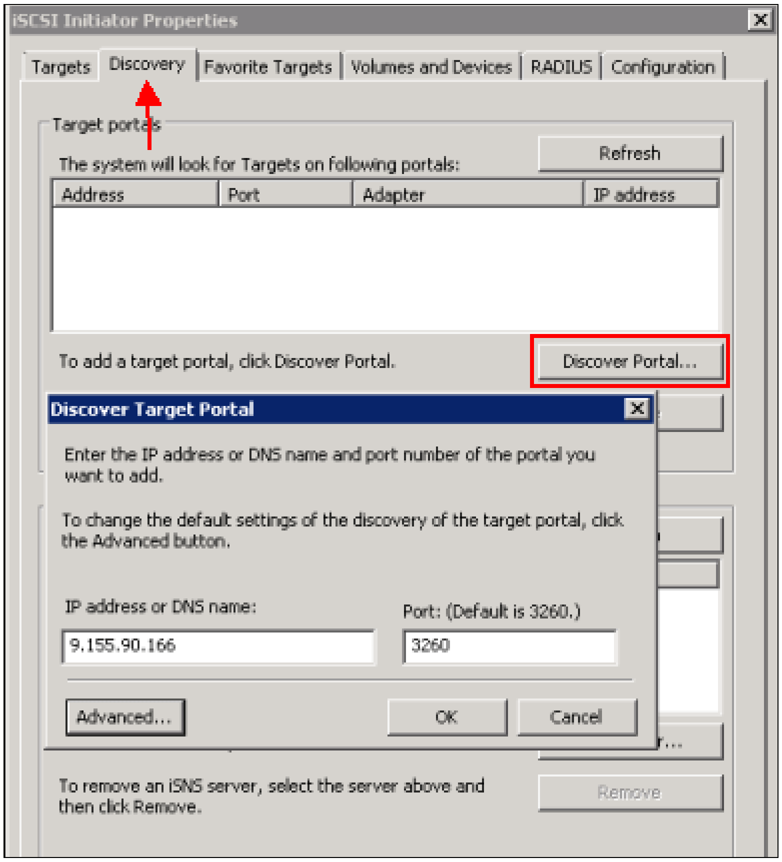



*Figure 7-47 Adding the storage iSCSI data interface*

7. Click **Targets**; the N series IQN will display as Inactive. Click **Connect**, as in Figure 7-48.

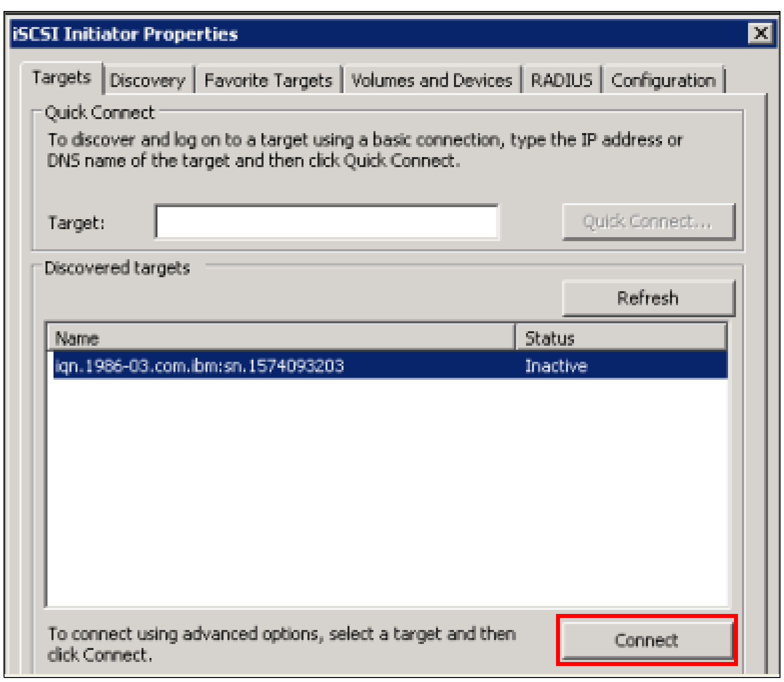



*Figure 7-48 Connect to the target iSCSI*

8. Accept the message and enable multipath if you have multiple NICs configured to access the storage. This choice is highly preferable. It changes the status to Connected.
9. Open Server Manager within that VM. Expand **Storage** and select **Disk Management**. The assigned LUN is shown there, as in Figure 7-49. If not, right-click **Disk Management** and select **Rescan**.

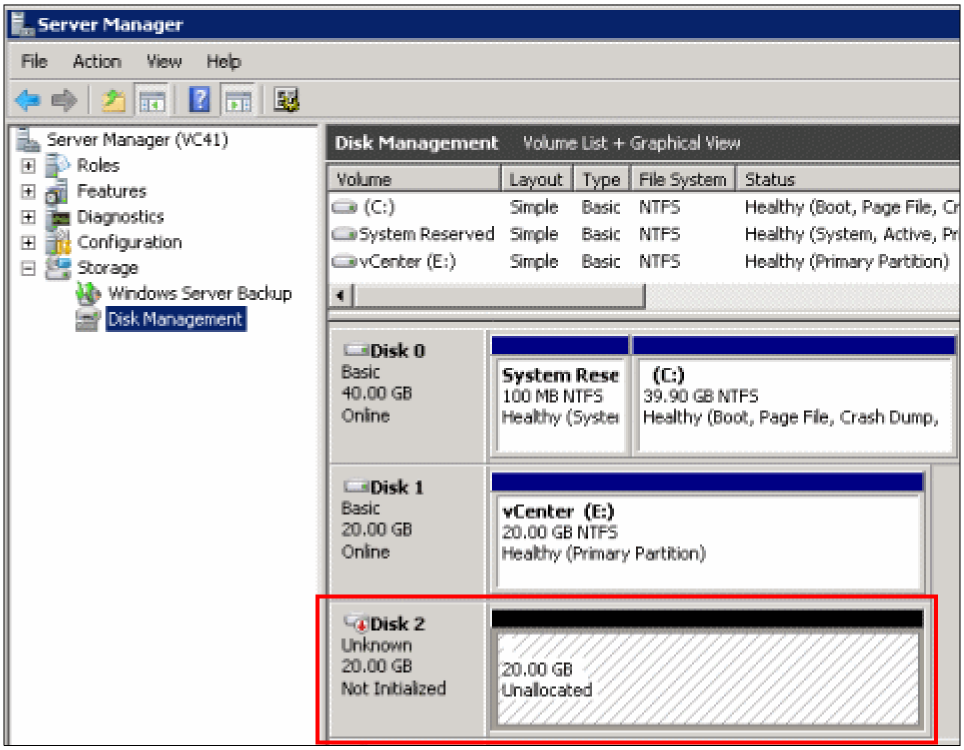



*Figure 7-49 The allocated LUN shows in Disk Management*

# 7.8 NFS volumes on VMware vSphere 4.1

NFS is widely used by server administrators due to its low cost and flexibility. An NFS volume can be increased (grown) and reduced (shrunk) at the N series level at any time without downtime.

This section explains how to set up an N series system for VMware ESXi host for NFS use.

## 7.8.1 Overview of NFS

With NFS, you have access to a volume hosted in a storage system over an Internet Protocol network. Servers can take advantage of NFS to mount storage volumes as though they were locally attached. An N series system and Virtual Infrastructure 3 support the use of NFS.

Virtual Infrastructure 3 requires the creation of a VMkernel switch for NFS. This is necessary because all the traffic between the storage system and the host must flow through the VMkernel virtual switch.

## 7.8.2 Setting up an NFS volume on N series

To make an NFS share available to an ESX host, follow these steps:

1. Create a volume structure in the N series system. We created an 80-GB volume named vol_nfs, as shown in Figure 7-50.

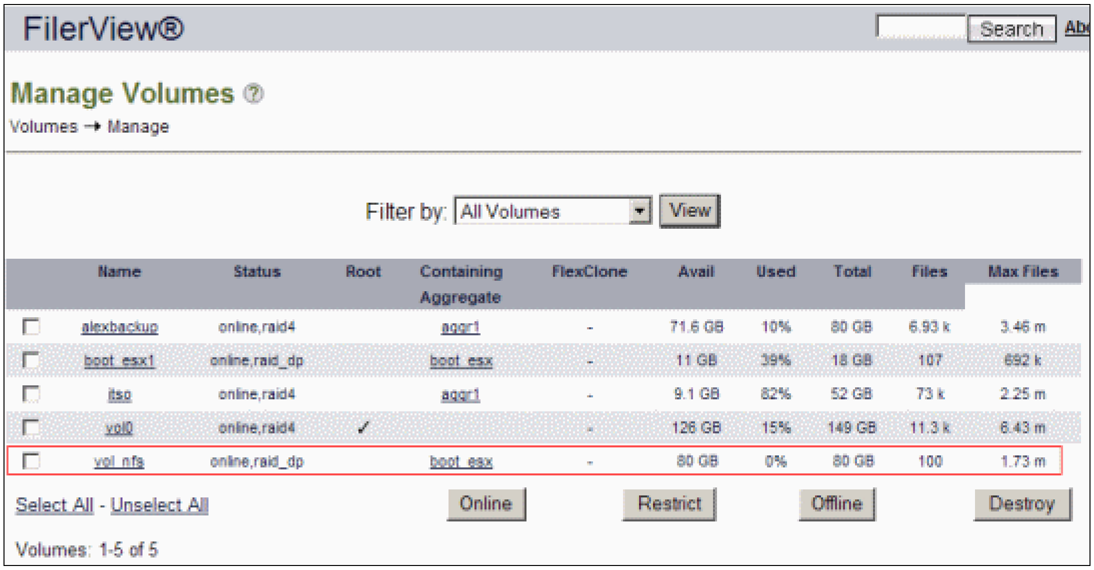



*Figure 7-50 Creating a volume structure*

2. After the volume is set up in the N series system, mount it in the VMware side:

   a. Using the Virtual Infrastructure Client (Figure 7-51), in the left pane, click the host you want to mount the NFS volume in. On the **Configuration** tab, under **Hardware**, select **Storage**. Then click **Add Storage**.

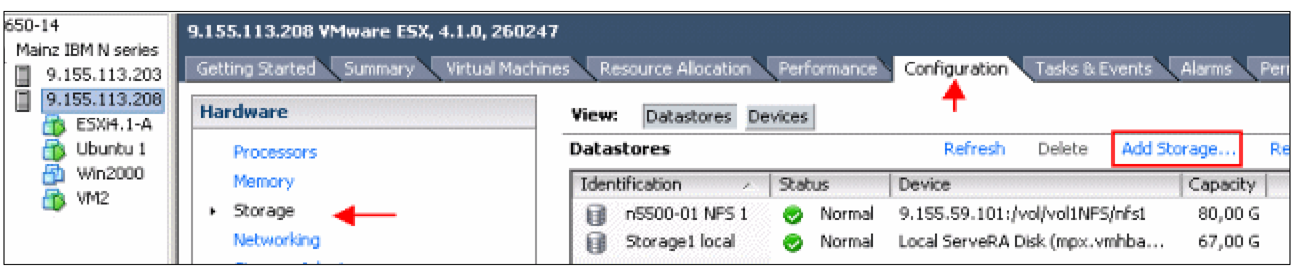



*Figure 7-51 Clicking the Add Storage... button*

3. In the Add Storage Wizard – Select Storage Type panel (Figure 7-52), click **Network File System**. Then click **Next**.

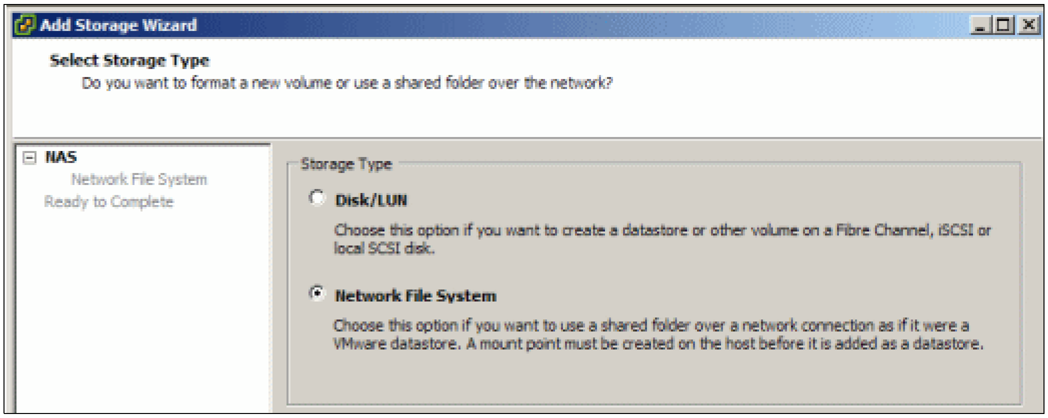



*Figure 7-52 Selecting the storage type*

4. In the Locate Network File System panel (Figure 7-53), complete these steps:
   i. Enter the storage system and volume name so that the ESX host can locate it.
   ii. Optional: Select **Mount NFS read only**, if your NFS volume is read only.
   iii. In the field Datastore Name, enter the display name of the NFS volume in the ESX host.
   iv. Click **Next**.

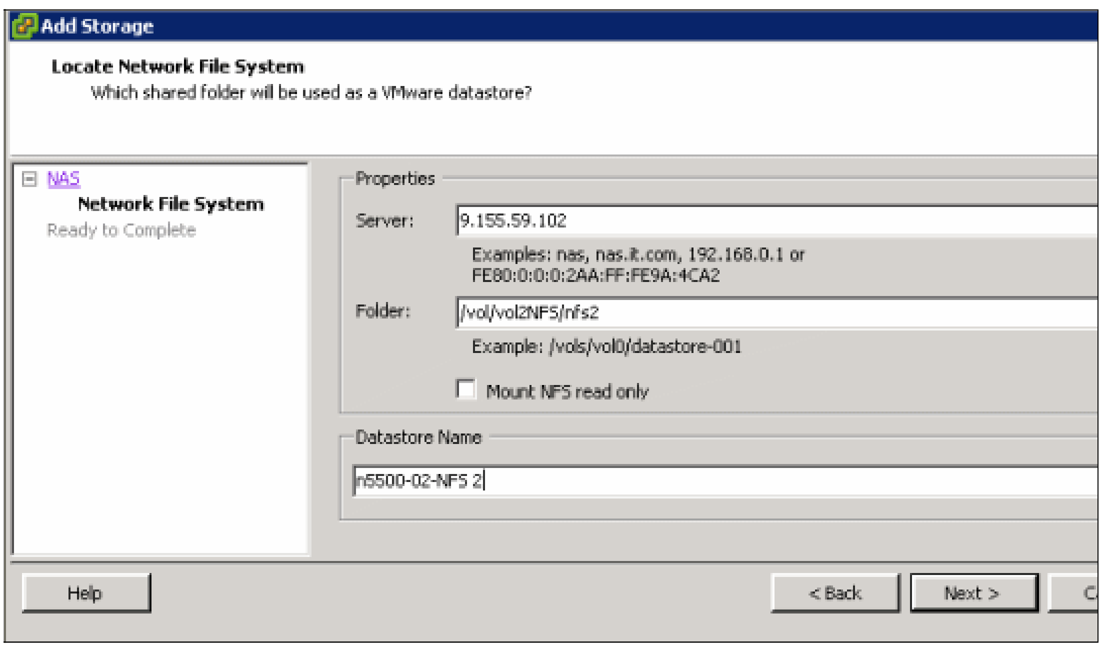



*Figure 7-53 Locating the network file system*

5. In the summary window, review the information provided and click **Finish**.

After the connection between the ESX host and the N series is established, the NFS volume is mounted, as shown in Figure 7-54. The NFS volume is now available as a new datastore in the VMware ESX host and is ready for use.

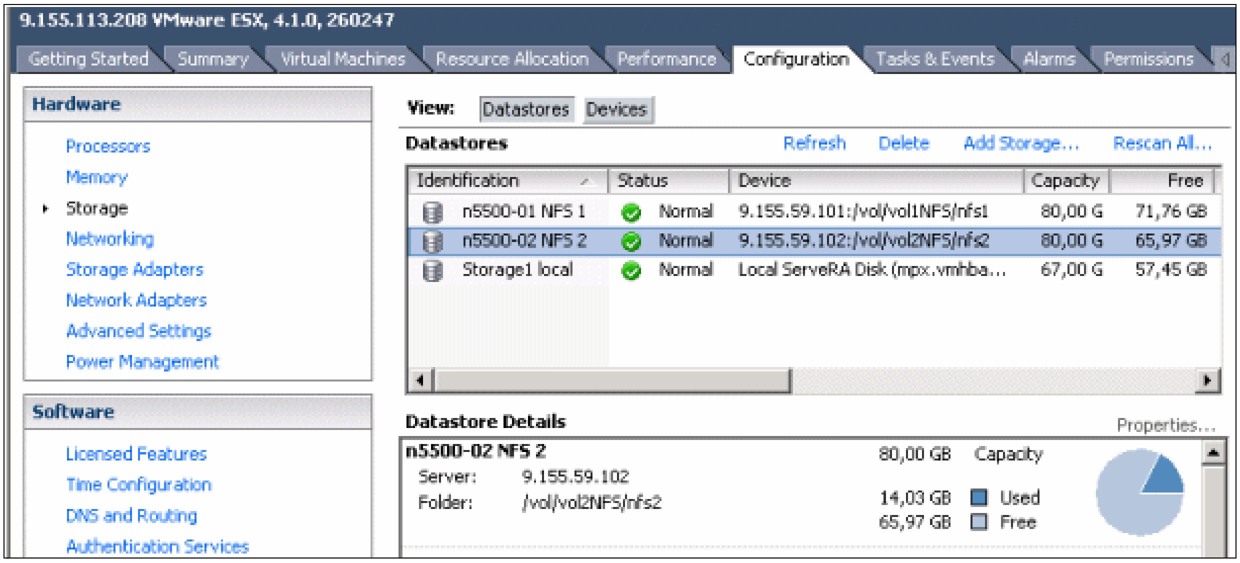


*Figure 7-54 Newly mounted NFS volume*

## 7.8.3 NFS datastore limits and options

By default, VMware ESX Server allows 8 NFS datastores. However, this limit can be increased to 64 to meet your infrastructure needs. To increase the value, perform the following steps from within the Virtual Infrastructure Client:

1. Open Virtual Center.
2. Select a host.
3. In the right pane, select the **Configuration** tab.
4. In the Software left box, select **Advanced Settings**.
5. In the Advanced Settings window (Figure 7-55), complete the following steps:
   a. Select **NFS** in the left pane.
   b. Change the value of NFS.MaxVolumes to 64.
   c. Change the value of NFS.HeartbeatFrequency to 12.
   d. Change the value of NFS.HeartbeatMaxFailures to 10.
   e. Select **Net** in the left pane.
   f. Change the value of Net.TcpIpHeapSize to 30. The change of this setting is implemented only after an ESXi server restart, so plan accordingly.
6. Repeat these steps for each host.

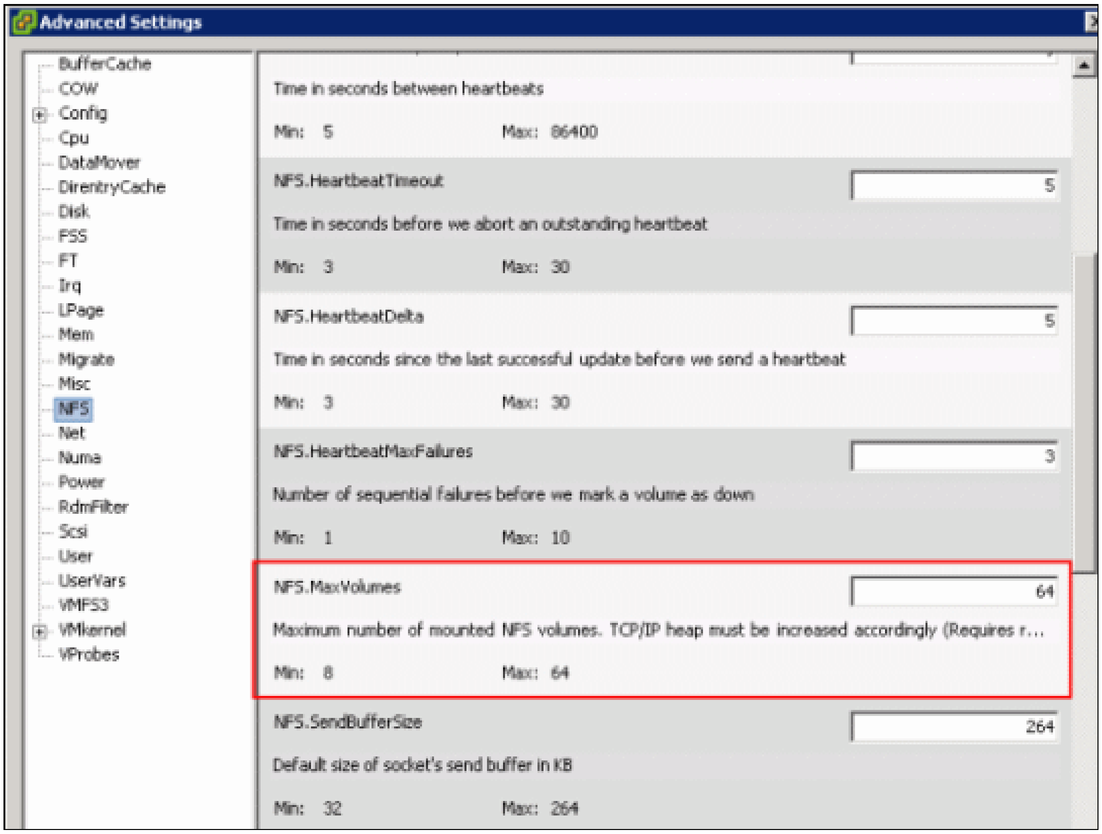



*Figure 7-55 Increasing NFS.MaxVolumes*

When deploying VMDKs on NFS, disable the access time updates that occur by default on the NFS. To disable the access time updates, log in to the N series console and run the following command:

```
vol options <vol-name> no_atime_update on
```

## 7.9 Partition alignment

In many cases, by default, a file system block is not aligned to the storage array. This type of alignment means that, for each random read or write, two blocks must be read or written. This situation can negatively impact the performance of the storage array. Sequential writes can also be affected, although to a lesser extent. Even when having a misaligned partition, performance degradation might not be noticed or reported, as it depends on the I/O load of each virtual machine. Misaligned guests with low I/O requirements might not justify the work to realign the disks.

In a non-virtualized environment, block alignment is done by selecting the appropriate LUN protocol type when the LUN is created. However, virtualization products, such as VMware, add another layer of complexity to alignment. In this situation, the VMFS datastore must be correctly aligned to the storage blocks, and the guest OS file system must be aligned with the other two layers. Misalignment of file systems is shown in Figure 7-56.

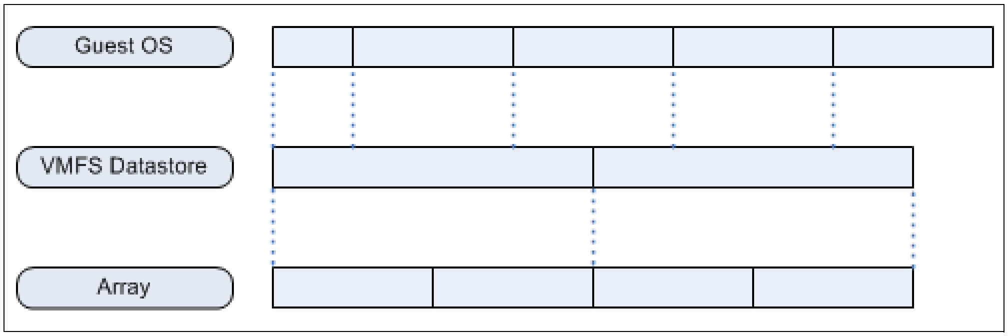



*Figure 7-56 Guest OS partition not aligned with VMFS and array partitions*

When aligning the partitions of virtual disks for use with N series storage systems, the starting partition offset must be divisible by 4096. The preferred starting offset value is 65,536.

On Windows servers, the misalignment problem occurs on versions running Windows 2003 and its predecessors. During the operating system installation, it creates the boot partition with a value slightly below 32KB - 32256 bytes (the correct value would be 32768 bytes). Thus, a mismatch occurs between the 4 KB physical block below it and the logical partition.

> **Tip:** Windows 2008 servers installed from scratch (not upgraded from 2003 servers) do not have this problem. The reason is that the aligned partitions are created either during the installation or later through the Disk Management interface.

To find the start offset of a partition on Windows, run `msinfo32` from a prompt command. Expand **Components**, **Storage**, then select **Disks**, and you typically find that the guest is running with a default starting offset value of 32256 (see Figure 7-57). It can occur if the partition was created through graphical interface, such as Microsoft Disk Management. Or it can occur if the boot partition was created automatically by Windows during its installation.

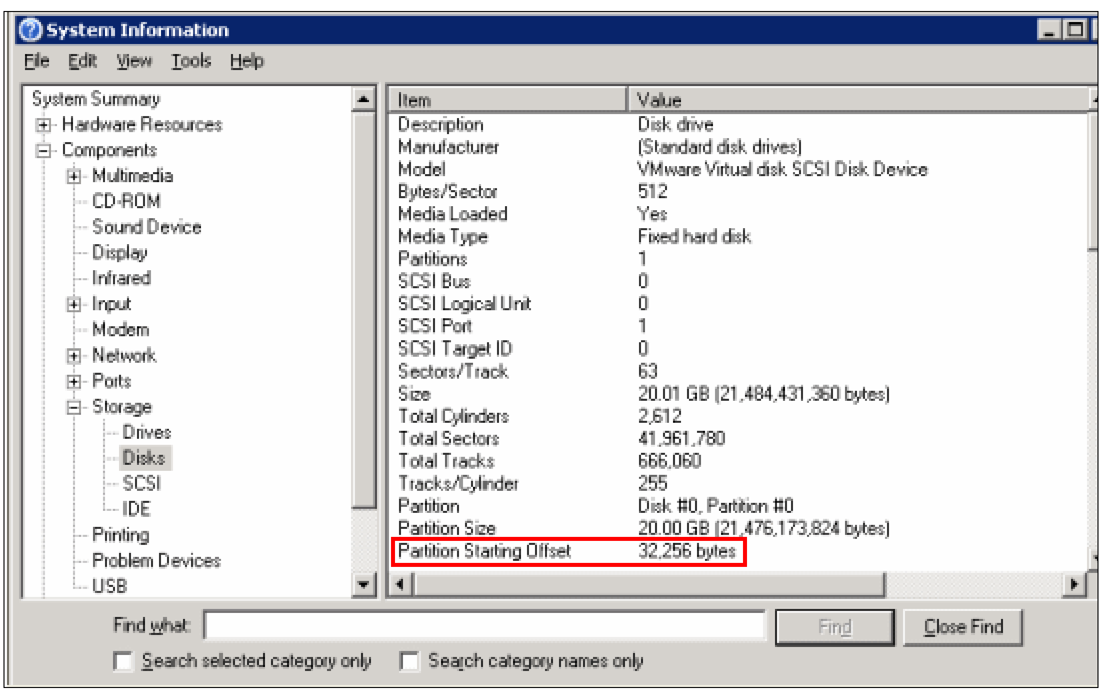



*Figure 7-57 Using system information to identify the partition starting offset*

Avoiding misalignment is better than correcting it later. So a best practice is to have aligned disks on your templates (which are virtual machine base images that are cloned to create new servers). Also, always create the Windows partitions through the **`diskpart`** command line utility.

> **Important:** Windows versions prior to 2008 always create misaligned partitions from the Disk Management graphical utility.

You can format a virtual disk with the correct offset at the time of its creation. Simply boot the guest *before* you install an operating system and manually set the partition offset. For Windows guest operating systems, the Windows Preinstall Environment boot CD is an excellent tool.

## 7.9.1 Creating an aligned partition on a Windows guest OS

This section explains how to create an aligned partition for a future guest OS installation. The aligned partition is saved as a template. Then it is used for all new deployments in the environment so that all new guest operating systems will have the correct alignment. This practice avoids a possible performance issue.

> **WinPE:** The following steps use a tool called WinPE to adjust the block alignment. WinPE is a bootable CD that has disk tools on it. In this case, we use the Diskpart tool to adjust the partition alignment of the virtual machine. For more information about WinPE and to download it, see the following website:
>
> `http://www.windowspe.com/`

To create an aligned partition for a future guest OS installation, follow these steps:

1. Create a standard virtual machine:
2. Mount the WinPE.iso file in CD/DVD drive 1 of the virtual machine. Select **Edit Settings** → **CD/DVD device 1** and browse the location of the WinPE.iso file. Make sure that the **Connect at power on** check box is selected.

3. Power on the virtual machine, which will boot through the WinPE.iso file, as shown in Figure 7-58.

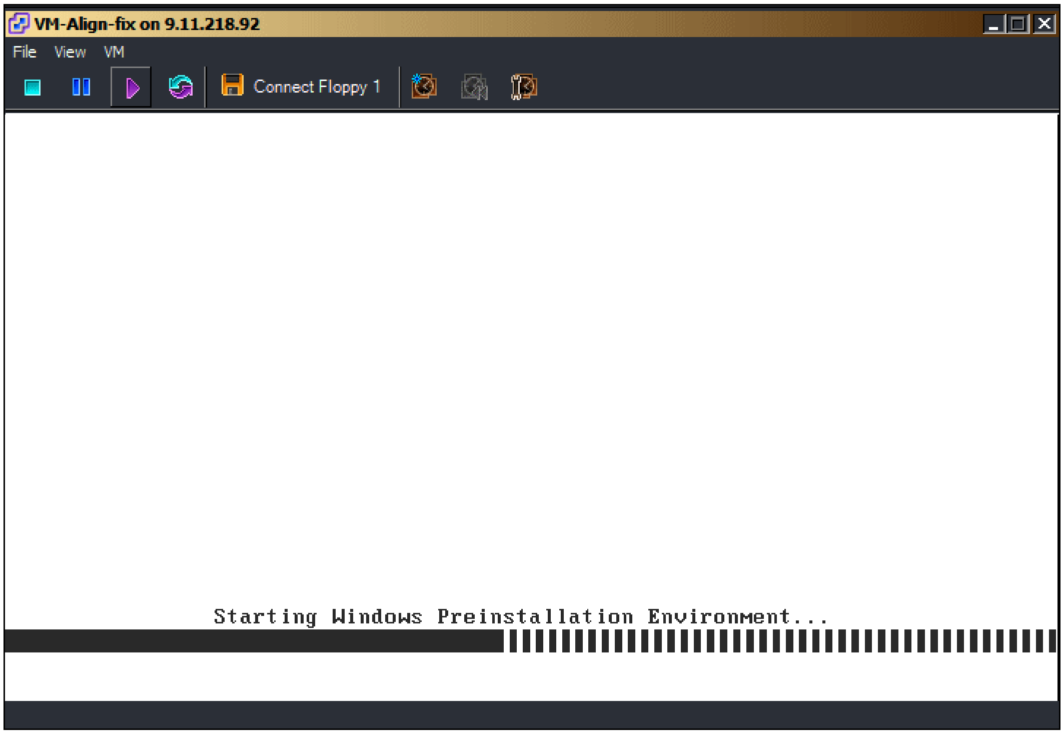



*Figure 7-58 Booting with the WinPE.iso file*

When the boot is complete, start the partition alignment from the command prompt that opens (Figure 7-59).

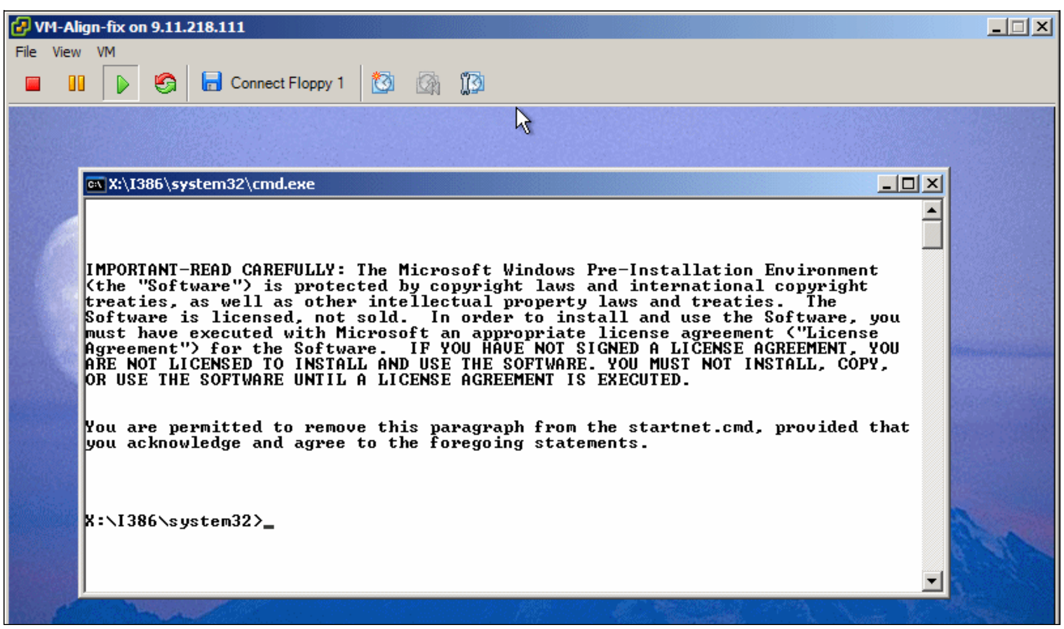



*Figure 7-59 Boot complete and command prompt available*

4. At the command prompt, issue the commands shown in Figure 7-60 to fix the partition alignment.

```
C:\> diskpart
DISKPART> list disk  (you might see only disk 0)
DISKPART> select disk 0
DISKPART> create partition primary align=64
```

*Figure 7-60 Diskpart commands*

5. Shut down the virtual machine and unmount the WinPE.iso file.

   Now the partition of the virtual machine disk is aligned and ready for the operating system installation.

   When creating data partitions after the OS install, use **diskpart**, which is included on Windows systems, with the same commands as shown in Figure 7-60.

> **Important:** Windows versions prior to 2008 always create misaligned partitions from Disk Management graphical utility, so use diskpart to create new partitions.

6. After the Microsoft operating system in installed and running, click **Start** → **Run** and type `msinfo32.exe`. In the left pane of the System Information window (Figure 7-61), expand **Components** → **Storage** → **Disk**. In the right pane, look for *Partition Starting Offset*, which must have a value of 65,536 bytes.

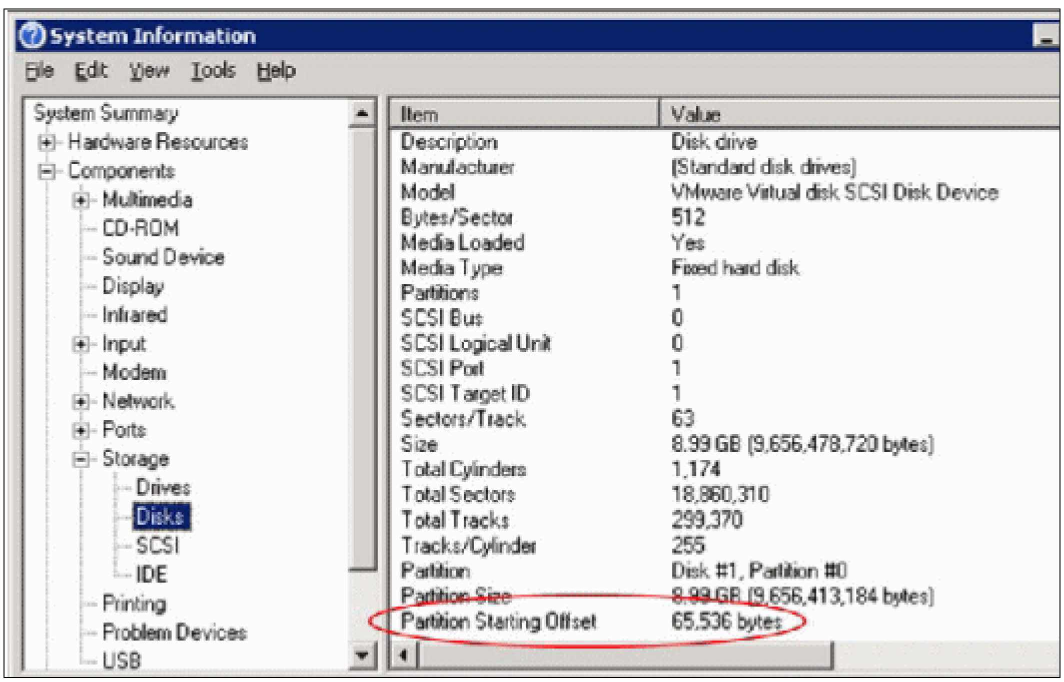



*Figure 7-61 Fixed partition alignment*

Now you can use this virtual machine with the correct partition aligned as a template for future guest operating systems deployment.

## 7.9.2 Realigning existing partitions

For disks that were created misaligned, you can use the **mbralign** and **mbrscan** utilities to realign the disk, without having to create a new disk and transfer all the data into it. These utilities are included in the host utility kit at the following website:

http://www.ibm.com/storage/support/nas

For currently running guests that are misaligned, correct the offset of only those guests that are experiencing I/O performance issues. The performance penalty is more noticeable on systems that are completing a large number of small read and write operations.

Although we advise using ESXi through the entire book, this command must be executed from an ESX host, because this version has a service console management to install.

The following steps show how to realign a partition misaligned by the operating system:

1. Make a backup of the disk that you want to align.
2. Download ESX Host Utilities 5.2.1 from this website:

   http://now.netapp.com/NOW/download/software/sanhost_esx/5.2.1/

3. Transfer it to your ESX server:

   a. Connect to your ESX host using Virtual Infrastructure Client.

   b. Select the **Configuration** tab, then in the **Hardware** panel on the left, choose **Storage**.

   c. Select one of the datastores listed, right-click it, and select **Browse Datastore...** as shown in Figure 7-62.

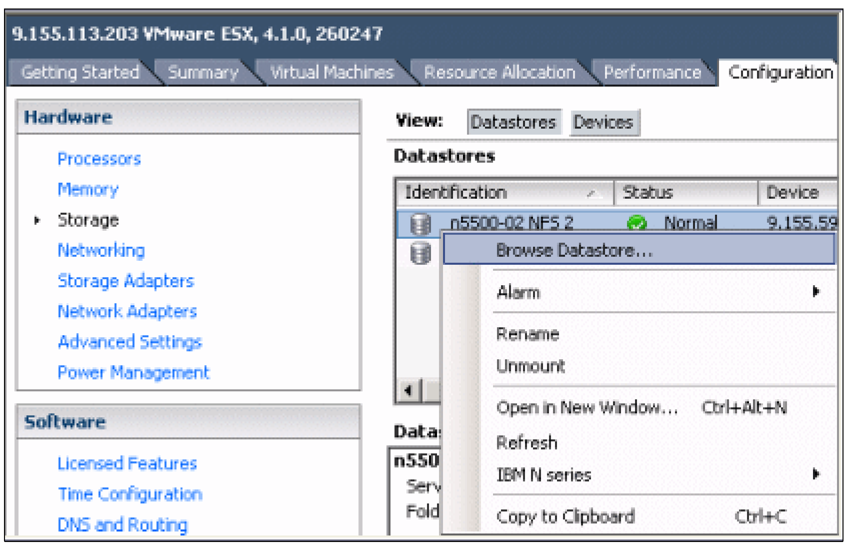



*Figure 7-62 Browse Datastore to upload/download files from your datastore*

   d. Select **Upload files to the datastore**, as shown in Figure 7-63.

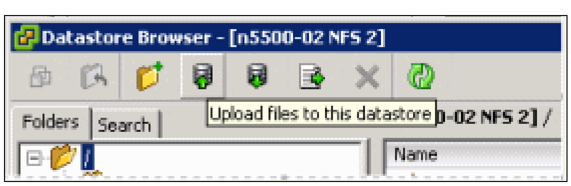



*Figure 7-63 Select Upload files to transfer data into your datastore*

   e. Browse your local disk to find the ESX Host Utilities downloaded and upload them to the datastore.

4. Unzip it running the command tar -xzvf netapp_esx_host_utilities_5_2.1.tar.gz
5. Change your directory to the santools: cd /opt/netapp/santools:

```
Check the alignment of a disk by running mbrscan and the full path of the disk:
[root@esx2 santools]# ./mbralign /vmfs/volumes/n5500-01NFS1/Win2000/Win2000.vmdk
```

6. You receive a message like this one; type **yes** and press Enter:

```
MBRAlign will align with a blocksize of 8 kB.
 Part    Type         Old LBA    New Start LBA      New End LBA     Length in KB
   P1      07              63               64         20948761         10474348

NOTICE:
This tool does not check for the existence of Virtual Machine snapshots or linked
clones.
The use of this tool on a vmdk file that has a snapshot or linked clone associated
with it
can result in unrecoverable data loss and/or data corruption.
Are you sure that no snapshots or linked clones exist for this vmdk file(s)?
(yes/no)
```

7. You need at least the same space of the virtual disk being aligned free on the datastore to complete the operation. Here is the output during the alignment:

```
Creating a backup of /vmfs/volumes/81eee9e4-8f38a96f/Win2000/Win2000.vmdk
Creating a backup of /vmfs/volumes/81eee9e4-8f38a96f/Win2000/Win2000-flat.vmdk
Creating a copy of the Master Boot Record
Working on partition P1 (3): Starting to migrate blocks from 32256 to 32768.
12801 read ops in 15 sec.  11.72% read (6.33 mB/s).  11.72% written (6.33 mB/s)
```

8. The results look like this example:

```
Working on space not in any partition: Starting to migrate blocks.
100.00 percent complete.  100.00 percent written. .
Making adjustments to /vmfs/volumes/81eee9e4-8f38a96f/Win2000/Win2000-flat.vmdk.
Adjusting the descriptor file.

Alignment complete for /vmfs/volumes/81eee9e4-8f38a96f/Win2000/Win2000.vmdk
```

9. The new Start LBA value is 64, showing that the disk is now aligned, and you are ready to start the virtual machine again.

# 7.10 Advanced guest operating system I/O configurations

This section explains tasks you can perform within the operating system of the guest systems.

## 7.10.1 Setting SCSI time-out values for N series failover events

To increase the resiliency of guests during storage failover events, modify the default SCSI disk time-out values within the guest operating system.

To modify these values in a Windows guest, follow these steps:

1. Connect to the virtual machine.
2. Open the registry editor.
3. Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk\TimeOutValue`.
4. Change the value to `190` (in decimal).
5. Close the registry editor.

## 7.10.2 Modifying the SCSI time-out value for RHEL4 (Kernel 2.6) guests

To modify the SCSI time-out value for RHEL4 (Kernel 2.6) guests, follow these steps:

1. Connect to the guest.
2. Log in as root.
3. Execute the following command:

   ```
   touch /sbin/scsi_disktimeout.sh
   ```

4. Edit the file from step 3 and enter the following content:

   ```
   #!/bin/bash
   for for device_dir in `ls -d /sys/block/sd*`
   do
      device_name=`basename ${device_dir}`
      echo "190" > /sys/block/${device_name}/device/timeout
   done
   ```

5. Execute the following command:

   ```
   chmod +x /sbin/scsi_disktimeout.sh
   ```

6. Execute the following command:

   ```
   touch /etc/udev/rules.d/52-nseries.rules
   ```

7. Edit the file from step 6 and enter the following content:

   ```
   BUS="scsi", PROGRAM="/sbin/scsi_timeout.sh"
   ```

8. Restart the udev by executing the following command:

   ```
   /sbin/udevstart
   ```

To modify the SCSI time-out value for Red Hat Enterprise Linux 5 guests, follow these steps:

1. Connect to the guest.
2. Log in as root.
3. Back up the udev file by running the following command:

   ```
   cp /etc/udev/rules.d/50-udev.rules /etc/udev/rules.d/50-udev.rules.orig
   ```

4. Edit the `/etc/udev/rules.d/50-udev-default.rules` file and modify the following line:

   ```
   ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", RUN+="/bin/sh -c
   'echo 60 > /sys$$DEVPATH/timeout'"
   ```

   Set the disk time-out value to 190 seconds:

   ```
   ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", RUN+="/bin/sh -c
   'echo 190 > /sys$$DEVPATH/timeout'"
   ```

5. Restart the udev file by executing the following command:

   ```
   /sbin/udevstart
   ```

To modify the SCSI time-out value for SUSE Linux Enterprise Server 9 (Kernel 2.6) guests, follow these steps:

1. Connect to the guest.
2. Log in as root.
3. Execute the following command:

   ```
   touch /sbin/udev.scsi_disktimeout.sh
   ```

4. Edit the file from step 3 and enter the following content:

   ```
   #!/lib/klibc/bin/sh
   for device_dir in `ls -d /sys/block/sd*`
   do
      device_name=`basename ${device_dir}`
      echo "190" > /sys/block/${device_name}/device/timeout
   done
   ```

5. Execute the following command:

   ```
   chmod +x /sbin/udev.scsi-disktimeout.sh
   ```

6. Copy the binary files referenced in step 4 by running the following command:

   ```
   cp /bin/ls  /lib/klibc/bin/ls
   cp /bin/echo  /lib/klibc/bin/echo
   cp /bin/basename  /lib/klibc/bin/basename
   ```

7. Back up the udev file by running the following command:

   ```
   cp /etc/udev/udev.rules /etc/udev/udev.rules.orig
   ```

8. Edit the `/etc/udev/udev.rules` file:

   a. Find the following line:

      ```
      "BUS="scsi", PROGRAM="/sbin/udev.get_persistent_device_name.sh", NAME="%k"
      SYMLINK="%c{1+}""
      ```

   b. Above this line, add the following line:

      ```
      KERNEL="sd*" PROGRAM="/sbin/udev.scsi_timeout.sh"
      ```

9. Restart the udev file by executing the following command:

   ```
   /sbin/udevstart
   ```

To modify the SCSI time-out value for SUSE Linux Enterprise Server 10 guests, follow these steps:

1. Connect to the guest.
2. Log in as root.
3. Back up the udev file by running the following command:

   ```
   cp /etc/udev/rules.d/50-udev-default.rules
   /etc/udev/rules.d/50-udev-default.rules.orig
   ```

4. Edit the /etc/udev/rules.d/50-udev-default.rules file:

   a. Modify the following line:

      ```
      ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", RUN+="/bin/sh -c
      'echo 60 > /sys$$DEVPATH/timeout'"
      ```

   b. Set the disk time-out value to 190 seconds:

      ```
      ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", RUN+="/bin/sh -c
      'echo 190 > /sys$$DEVPATH/timeout'"
      ```

5. Restart the udev file by executing the following command:

```
/etc/init.d/boot.udev force-reload
```

To modify the SCSI time-out value for Solaris 10 x86 guests, follow these steps:

1. Connect to the guest.
2. Log in as root.
3. Back up the /etc/system file by running the following command:

```
cp /etc/system /etc/system.orig
```

4. Add the following line to the /etc/system file:

```
set sd:sd_io_time=0xbe
```

5. Restart the virtual machine.

# 7.11 Monitoring and management

This section provides information about monitoring and managing the IBM System Storage N series storage system.

## 7.11.1 Monitoring storage utilization with Operations Manager

IBM offers the Operations Manager product to monitor, manage, and generate reports on all of the IBM System Storage N series systems in an organization. When you are using N series thin provisioning, deploy Operations Manager and set up email and pager notifications to the appropriate administrators. With thin provisioned storage, it is important to monitor the free space that is available in storage aggregates. Proper notification of the available free space ensures that additional storage can be made available before the aggregate becomes full.

## 7.11.2 Setting up notifications in Operations Manager

For more information about setting up notifications in the version of Operations Manager you are using, see the *Operations Manager Administration Guide* at this website:

https://www-304.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5345868

**Access to IBM Systems support:** You must register for access to IBM Systems support applications and content. You can register at the following address:

https://www-304.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=REGS-NAS&brandind=5345868

# 7.12 Storage growth management

This section explains growing the different storage components that make up the datacenter.

## 7.12.1 Growing VMFS volumes

Beginning on vSphere 4, VMFS growing on the fly is supported, which means that you can grow your datastore with all VMs running without any disruption.

To grow a datastore, follow these steps:

1. Open FilerView:

   `http://Nseries/na_admin`

2. Select **LUNs**.
3. Select **Manage**.
4. In the left pane, select the LUN from the list.
5. Enter the new size of the LUN in the Size box and click **Apply** (Figure 7-64).

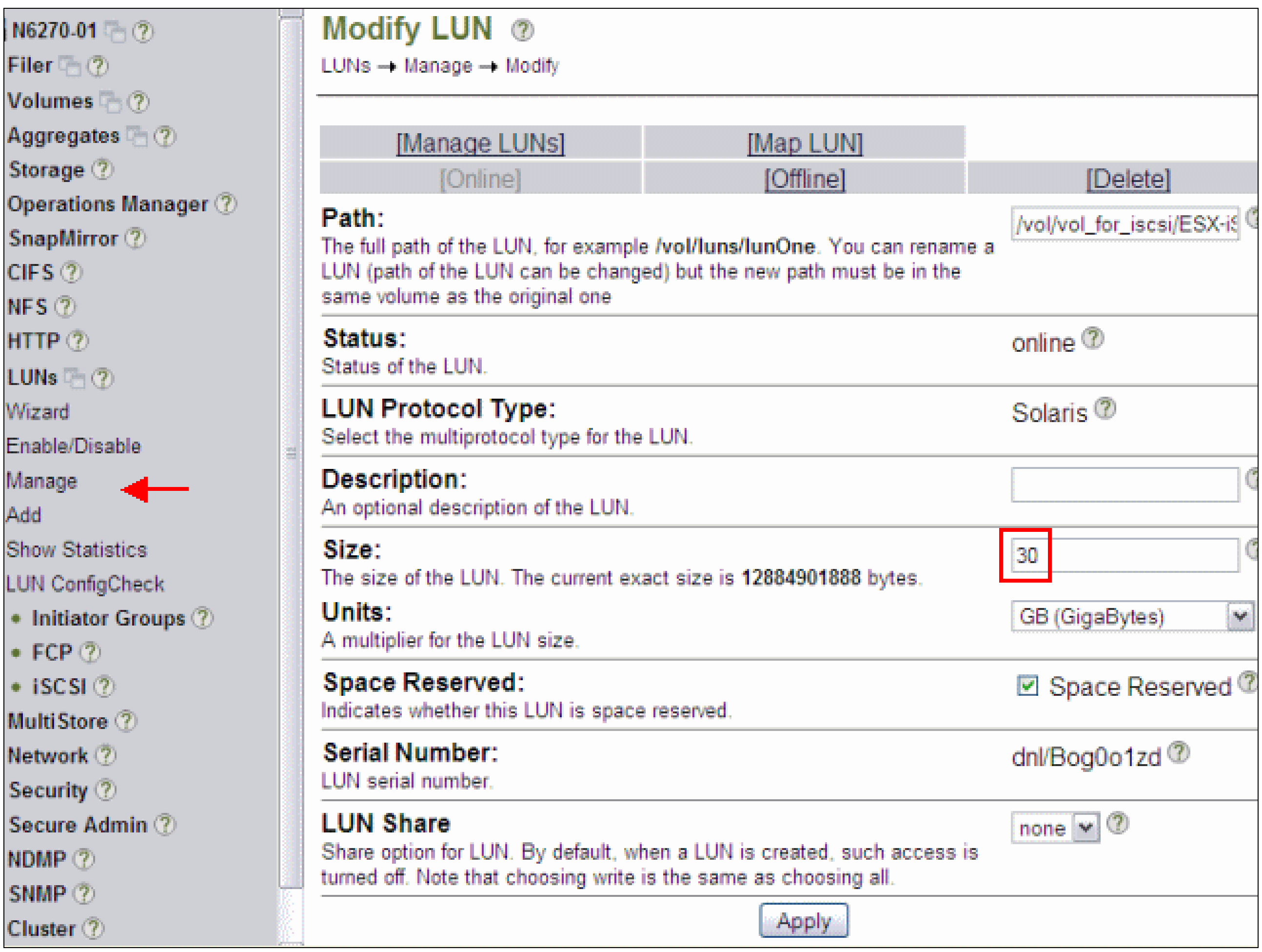



*Figure 7-64 Expanding a LUN*

6. Open vCenter.
7. Select a host.
8. In the right pane, select the **Configuration** tab.
9. In the Hardware box, select the **Storage**, then click **Rescan All.**
10. After the rescan, right-click and select the datastore that you want to grow and then select **Properties**.
11. When you see the new size of the LUN right next to the red array, now the datastore has to be extended to that size. Click **Increase** on the left upper corner, as in Figure 7-65.

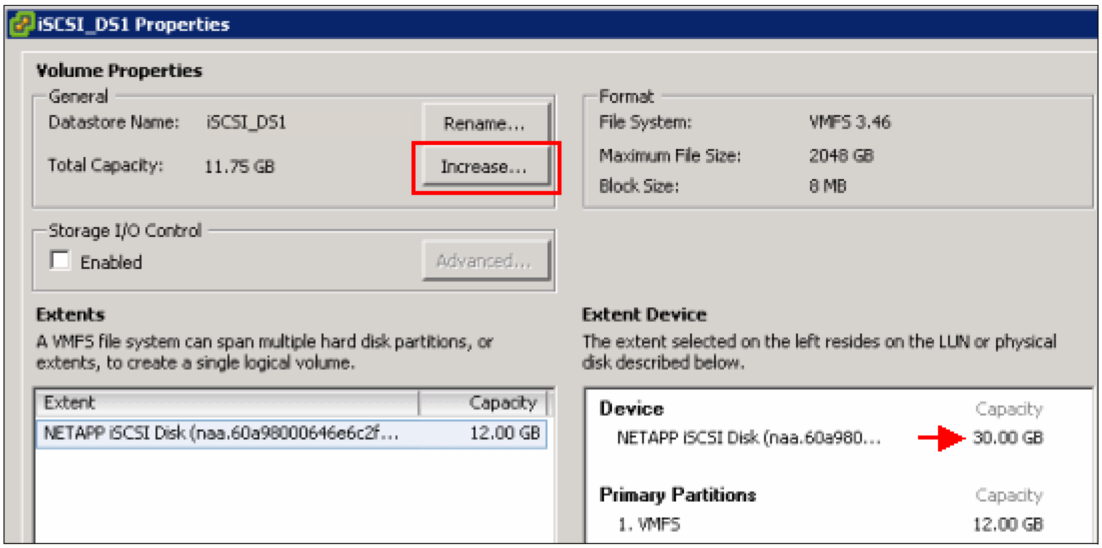


*Figure 7-65 Increasing datastore capacity*

12. When you see the new expanded LUN, select it and click **Next**, as in Figure 7-66.

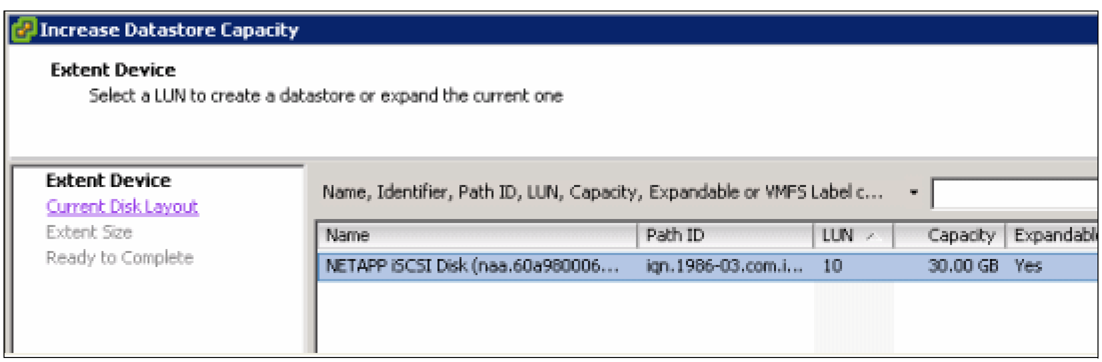


*Figure 7-66 Extended LUN*

13.When the new structure is shown, click **Next** (Figure 7-67).

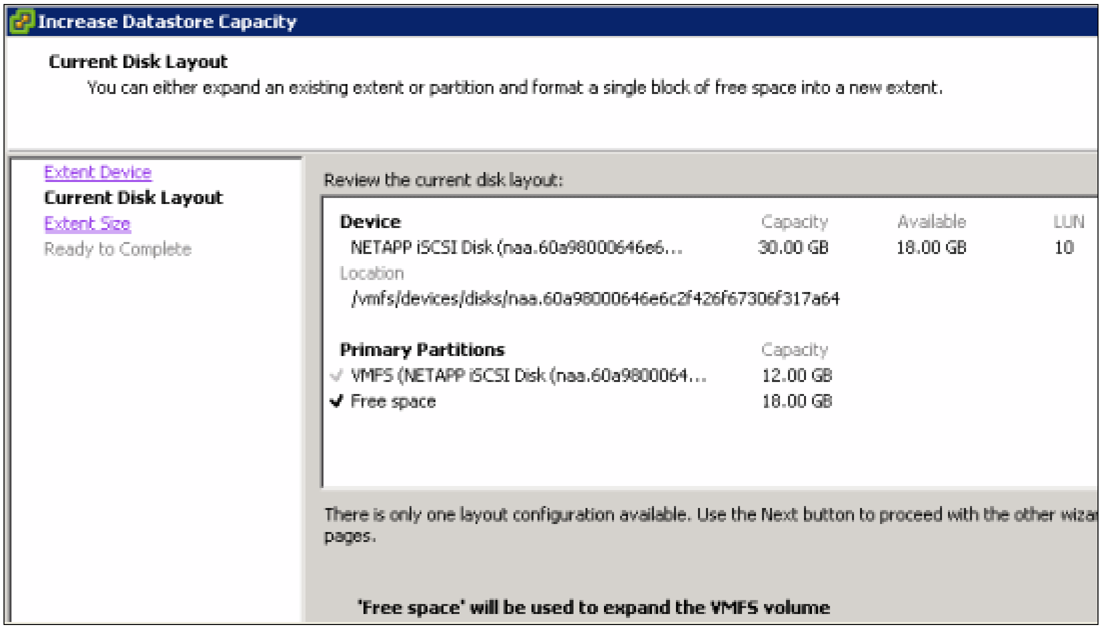


*Figure 7-67 New datastore structure*

14.Mark the box to expand the datastore to the maximum size of the LUN and click **Next**.

15.Review the new datastore structure and click **Finish**.

16.Check the new values of your datastore by clicking it, as in Figure 7-68.

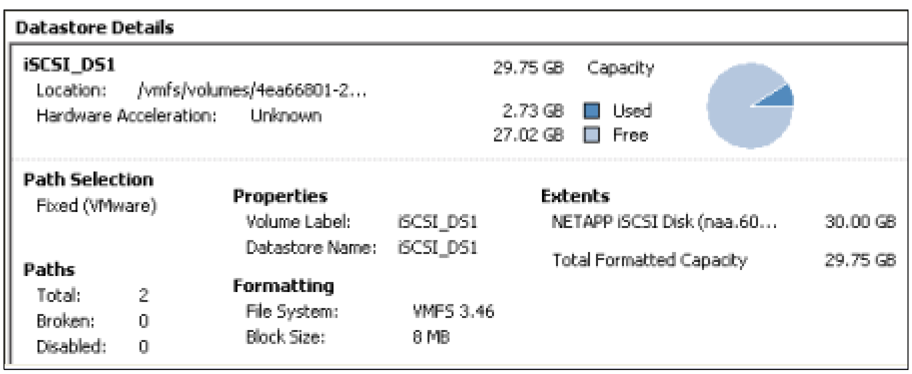


*Figure 7-68 The new values for the expanded datastore*

## 7.12.2 Growing a virtual disk

In an analog way to Datastores, Virtual disks can be extended while the VM is running.

However, growing the virtual disk is only half of the equation to increasing available storage. You still need to grow the file system after the guest boots. Root volumes, such as C:\ in Windows and / in Linux, cannot be grown dynamically or while the system is running. For these volumes, see "Growing bootable volumes" on page 151.

For all other volumes, you can use native operating system tools to grow the volume. To grow a virtual disk, follow these steps:

1. Open vCenter.
2. Right-click the desired Virtual Machine and select **Properties**.
3. Select a virtual disk, and in the right pane, increase its size, as shown in Figure 7-69. Then click **OK**.

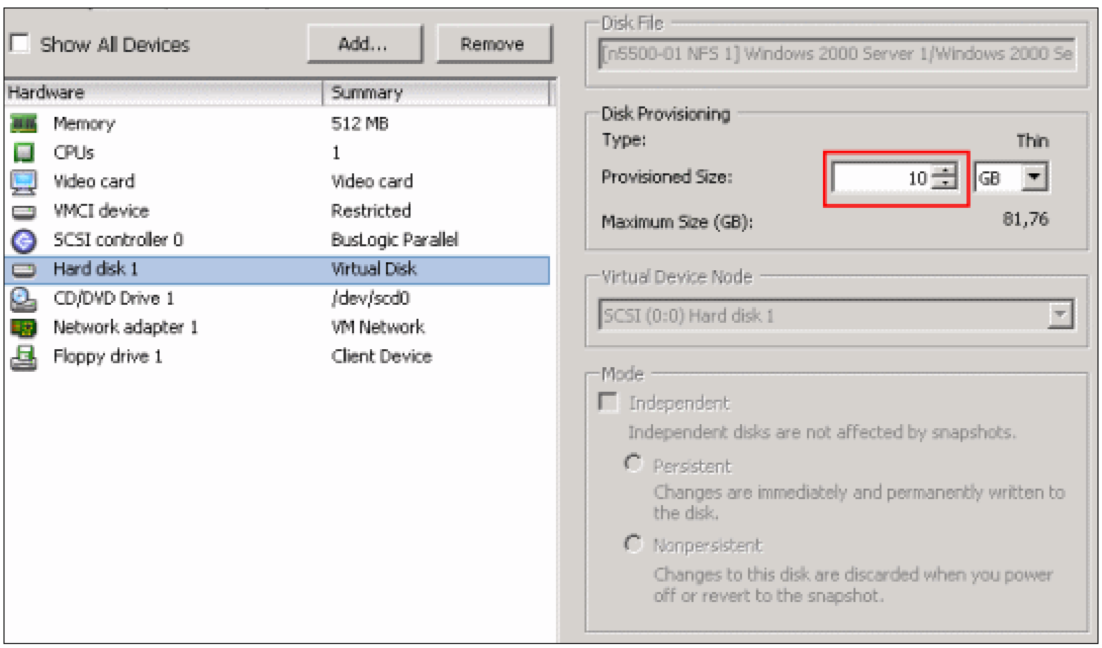



*Figure 7-69 Growing a virtual disk*

## 7.12.3 Growing an RDM

Growing an RDM has components of growing a VMFS and a virtual disk. This process requires the guest to be powered off. To grow RDM-based storage, follow these steps:

1. Open vCenter.
2. Right-click the desired Virtual Machine and select **Edit Settings**.
3. Highlight the hard disk to be resized, and click **Remove**.
4. As shown in, select **Remove from virtual machine and delete files from disk** to delete the mapping file. However this option does not remove any data from the RDM LUN. Then click **OK**.
5. Open FilerView:

   `http://Nseries/na_admin`

6. Select **LUNs**.
7. Select **Manage**.
8. From the list in the left pane, select the LUN.
9. In the Size box, enter the new size of the LUN and click **Apply**.
10. Return to vCenter.
11. In the right pane, select the **Configuration** tab.
12. In the Hardware box, select the **Storage,** then click the **Rescan All...**
13. Right-click the guest and select **Edit Settings** to open the Edit Settings window.
14. In the next panel, highlight **Select a Disk**, and in the right pane, select **Raw Device Mappings**. Then click **Next**.
15. In the Select and Configure a Raw LUN panel, select the LUN and click **Next**.
16. Specify the VMFS datastore that will store the mapping file.
17. Start the guest. Remember that, although you have grown the LUN, you still need to grow the file system within it. Follow the guidelines in the next section, "Expanding the guest file system (NTFS or EXT3)".

## 7.12.4 Expanding the guest file system (NTFS or EXT3)

When a virtual disk or RDM has been increased in size, you still need to grow the file system that resides on it after booting the guest.

### Growing the file system

You can perform this process live while the system is running by using native or freely distributed tools:

1. Remotely connect to the guest.
2. Grow the file system.

   For Windows guests, you can use the **`diskpart`** utility to grow the file system. For more information, see the topic "A Description of the Diskpart Command-Line Utility":

   `http://support.microsoft.com/default.aspx?scid=kb;en-us;300415`

   For Linux guests, you can use **`ext2resize`** to grow a file system. For more information, see the following web page from SourceForge:

   `http://sourceforge.net/projects/ext2resize`

## Growing bootable volumes

Root volumes, such as C:\ in Windows guests and / in Linux guests, cannot be grown while the guest is running. However, you can expand these file systems in a way that does not require the acquisition of any additional software beyond **`ext2resize`**. This process requires the VMDK or LUN that has been resized to be connected to another guest of the same operating system type, by using the processes defined in "Growing a virtual disk" on page 149:

1. Shut down the Virtual Machine that has the disk to be expanded, for this example, VM1.
2. Add the virtual disk containing the boot volume of VM1 to another VM, in this example, VM2.
3. Rescan the disks on Disk Management from Windows, and the new added disk will display. It shows as a disk with 1 GB of free space, as in Figure 7-70.

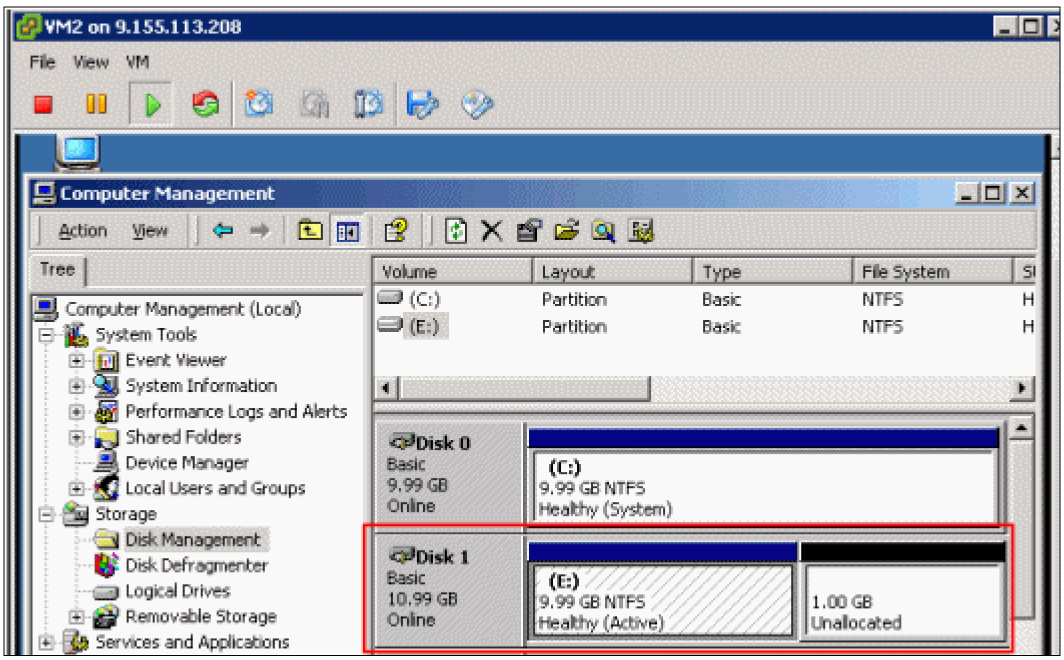



*Figure 7-70 System drive attached to another VM in order to be increased a a normal drive*

4. Extend it as a normal disk.
5. Shut down the VM, detach the virtual disk, and read it to the original VM.
6. Start the original VM and check if the partition was extended accordingly.

# 8

# N series cloning

This chapter provides information about the best ways to use N series cloning technologies with VMware vSphere 4.1. It includes the following topics:

- VMware and N series cloning technologies
- Cloning guests within a datastore
- Cloning an entire datastore
- Cloning VMware ESXi servers

## 8.1 VMware and N series cloning technologies

Cloning virtual machines is a feature available with VMware for years. Cloning consists in copying all the files containing in a VM. These files are virtual disks (.vmdk), configuration files (.vmx), BIOS configuration (nvram), and logs (.log). Cloning results in a new guest, with the exact same configuration of its parent, but running independently from the virtual machine that originated it.

By applying that concept, you can create a template, also known as a “golden image,” of a base server, with all the tools that are server name and IP agnostic. You then use it to provision new servers for building up your environment.

### 8.1.1 Provisioning new servers

N series FlexClone can also be used to provision new servers. If you have a traditional VMFS file system in a Fibre Channel environment, FlexClone does not offer a significant advantage over the native VMware cloning feature. However, if you are using NFS, FlexClone offers the benefit of performing the clone procedure from the storage side, reducing the load on the VMware side. Also, if using RDMs, you can clone them using a LUN clone and then split the LUN clone, which also removes the load from the VMware host.

So far, none of these cloning solutions save storage space. The real value of FlexClone (Figure 8-1) in a virtual infrastructure is realized when you use it to create temporary guests. It is beneficial for creating a large number of guests to provision a test and development center, a demonstration center, or a training center, and when you need 30 guests for testing. In a traditional VMware environment, that operation would take 30 times the clone of the original machine. You must wait while that data copies 30 times. Obviously, it can be expensive to provision large numbers of guests in such a traditional environment.

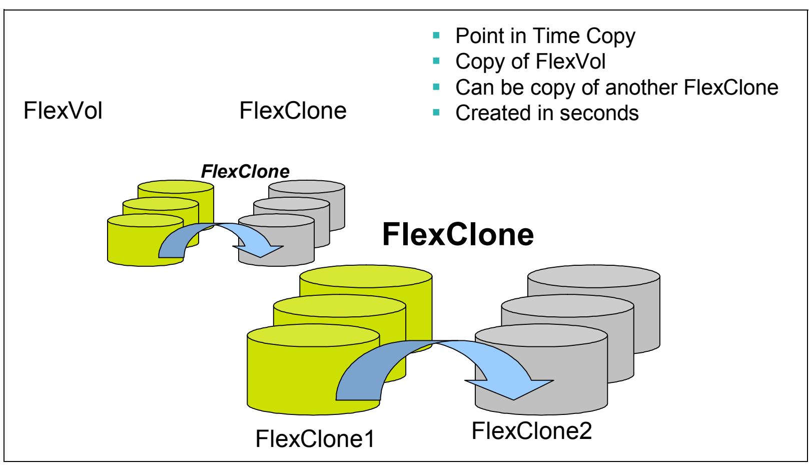



*Figure 8-1 FlexClone*

## 8.1.2 Cloning individual virtual machines

You can use the N series FlexClone or LUN clone feature to quickly provision a large number of virtual disks on N series storage systems. You then attach new guests to the cloned drives. Because of the N series cloning technology, the storage space consumed by the cloned virtual disks is only a fraction of the space that another storage system might use. You might need many guests, or are constantly creating and recreating temporary guests. N series FlexClone or LUN clone technology provides significant space savings while dramatically reducing the time needed to complete the cloning process.

In such situations, the N series storage virtualization technologies can play a key role in guest deployments.

To clone a large number of guests, follow these steps:

1. Build a datastore and create a virtual machine to be the prototype for the cloned guests. For Windows systems, use Sysprep to ensure that, when the guests are cloned, they are recognized by the operating system as unique systems.
2. Take a Snapshot of that datastore, and create a FlexClone. You do not want to use the original copy in case something goes wrong. Then mount the FlexVol on the VMware ESXi Server.
3. Using VMware vSphere, create clones of the original virtual machine in that datastore. You can create as many clones as you want, taking in consideration the datastore size and your needs. Figure 8-2 shows six guest systems. In this example, you have a datastore that contains multiple clones of the original guest system.

You can also run the N series Advanced Single Instance Storage (A-SIS) feature on the datastore to reduce the consumed storage space back down to the size of the original guest.

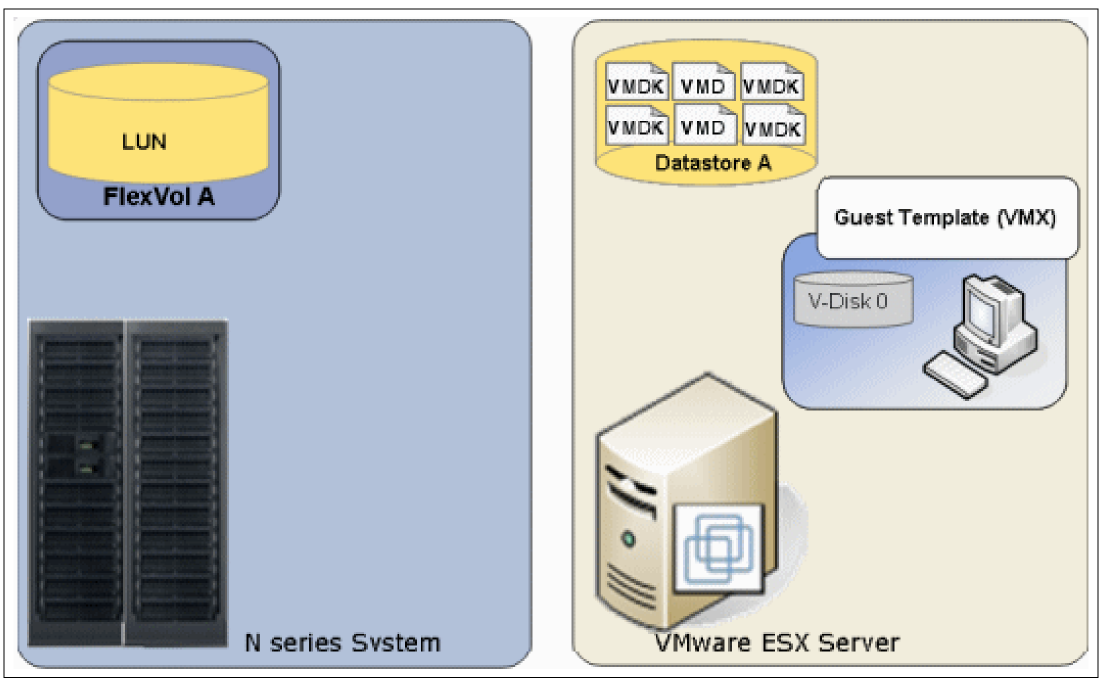



*Figure 8-2 A datastore with six cloned guests*

4. Use N series to create FlexClones of the initial FlexVol that contains the datastore where the cloned virtual machines reside.
5. After the FlexClones are created (Figure 8-3), add the datastores to the VMware hosts, register the virtual machines in the vCenter and start them. You can write a script to boot the guests in an orderly fashion, so that you do not overburden the VMware hosts. You are done. You went from one to many guests without consuming any additional storage; you did it quickly, and you can repeat the process at any time.

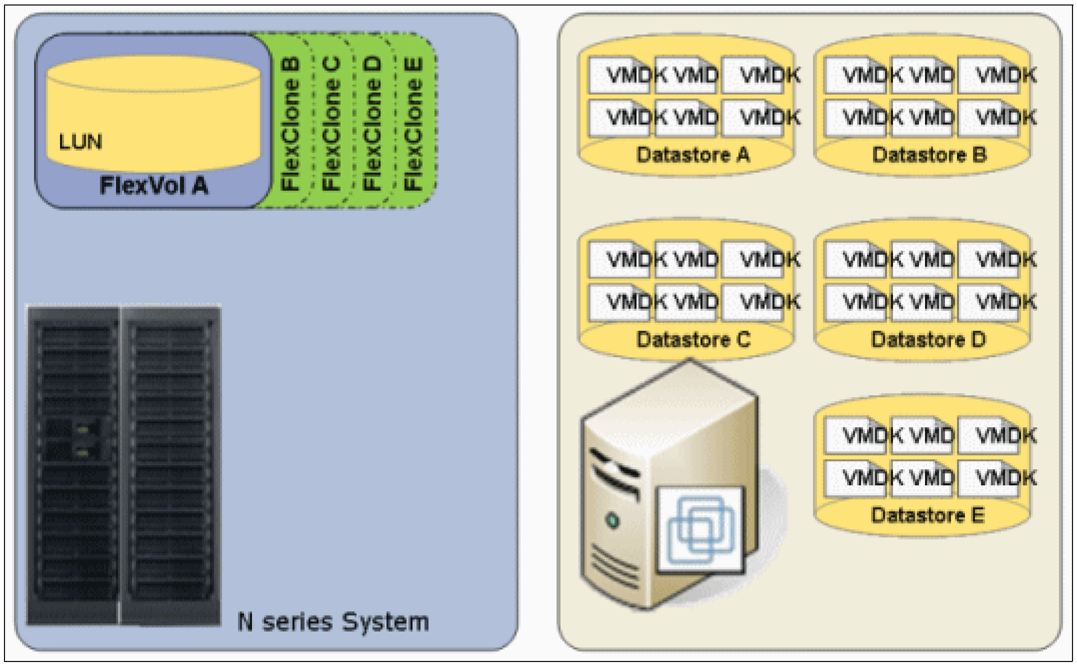



*Figure 8-3 Virtual infrastructure with four quickly deployed, space-efficient datastores*

## 8.2 Cloning guests within a datastore

To clone a guest by using VMware, follow these steps:

1. In the left pane of the VMware Infrastructure Client (Figure 8-4), right-click the guest you want to clone, and click **Clone**.

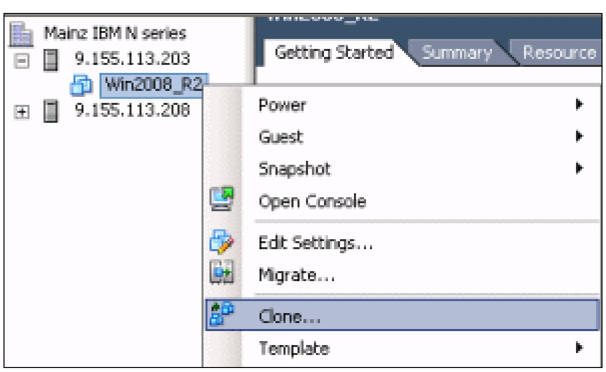



*Figure 8-4 Cloning a virtual machine*

2. In the Clone Virtual Machine Wizard shown in Figure 8-5, specify the name for your clone, and select the data center in which to place the cloned guest. Then click **Next**.

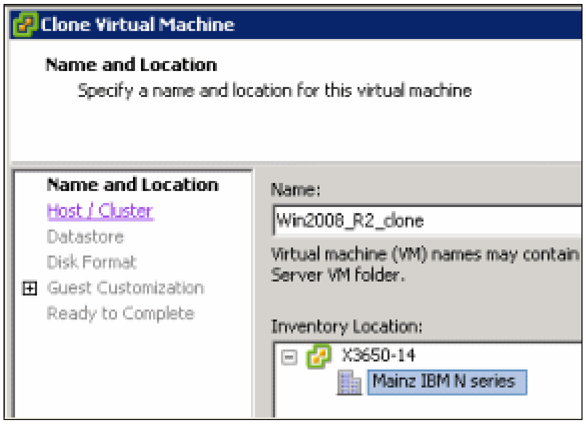



*Figure 8-5   Enter a name for the new server*

3. In the Specify a Specific Host panel (Figure 8-6), review the details about the capability of the host to run the guest you are cloning. If no changes are necessary, click **Next**.

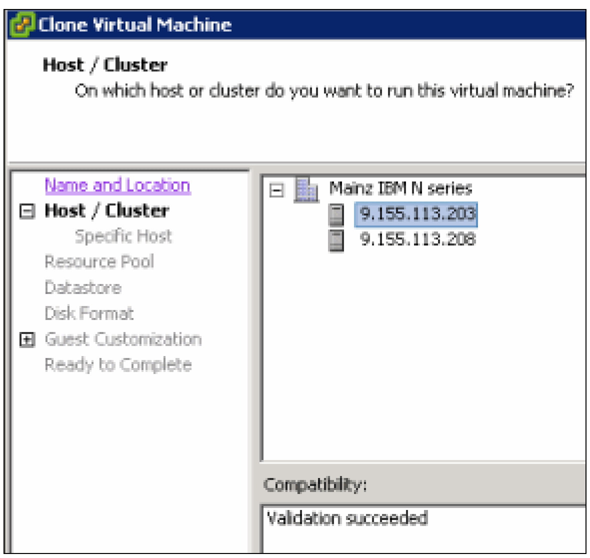



*Figure 8-6   Selecting a host and check if the validation succeeded*

4. In the Choose a Datastore for the Virtual Machine panel (Figure 8-7), select a datastore for the cloned guest. Additionally, click **Advanced**, and select specific datastores for each file of the guest. It is a best practice for easy maintenance to keep everything together in a single datastore. After you make your selection, click **Next**.

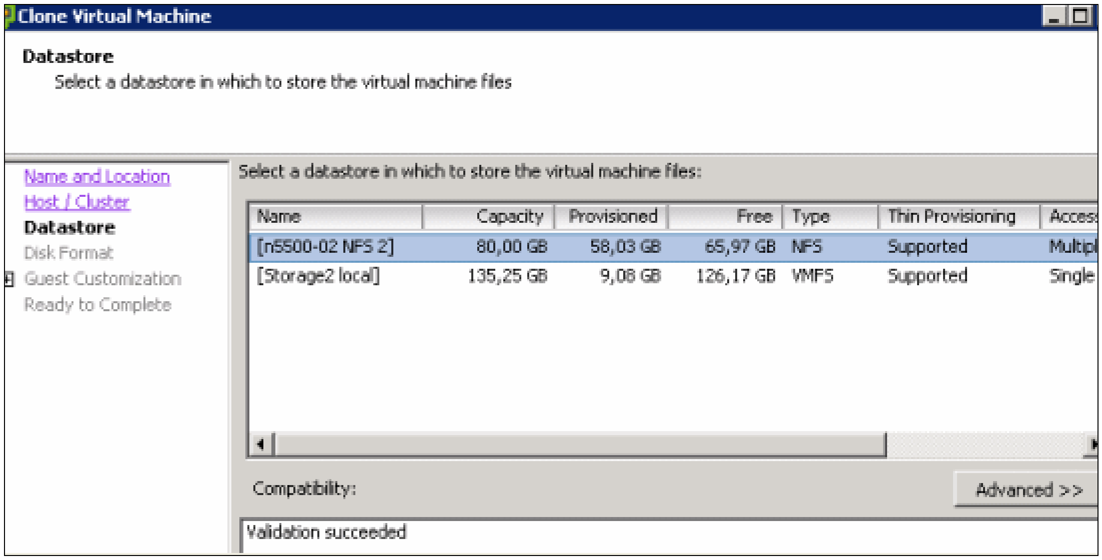



*Figure 8-7 Selecting a datastore*

5. In the Select Guest Customization Option panel, select the **Do not customize** radio button. Although you can have Sysprep attached to the cloned guest so that it can be made a new system when starting, it is not in the scope of the topic of this chapter. Then click **Next**.
6. On the Disk Format panel, you can select to keep the cloned disks in the same format as the source, have them Thin provisioned or Thick provisioned. We kept the same format, as in Figure 8-8, and clicked **Next**.

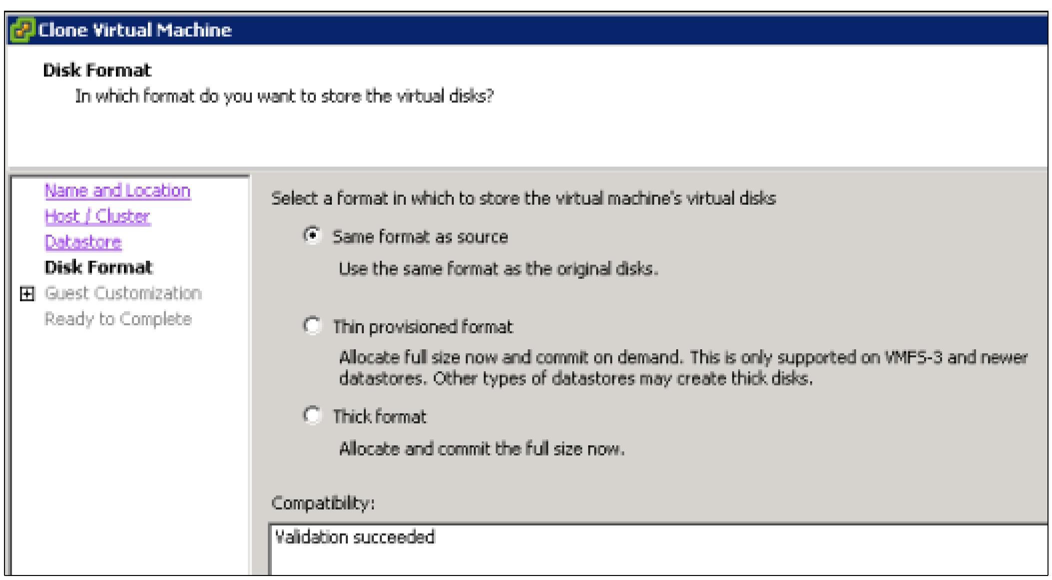



*Figure 8-8 Selecting the disk format, as Thin, Thick or the same as the source*

7. In the Ready to Complete New Virtual Machine window, in Figure 8-9, confirm all of your selections. Then decide if the guest must power on after the copy has completed, or if you need to edit the virtual hardware. Then click **Finish**.

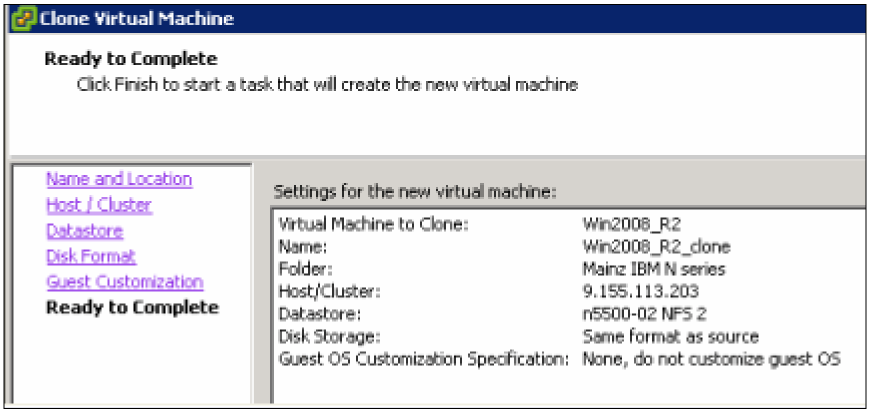



*Figure 8-9 Verifying the options to create a new cloned virtual machine*

8. After the Clone Virtual Machine is completed on the Recent Tasks pane of the vCenter, you will have your clone as shown in Figure 8-10. It is ready to be started and modified as necessary.

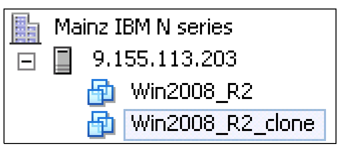



*Figure 8-10 Cloned VM ready to be used*

## 8.3 Cloning an entire datastore

To clone a datastore with multiple guests in it, follow these steps:

1. Ensure that all guests within the datastore are powered off so that the clone of the datastore is in a consistent state, as in Figure 8-11.


*Figure 8-11 All the virtual machines within the datastore are down*

2. To clone a LUN and assign it to an Initiator Group containing your VMWare hosts, see the following the procedures:
   - 10.2.1, “Creating a clone” on page 180
   - 10.2.2, “Configuring the cloned LUN to be accessed” on page 183
3. Back in the vCenter, on the **Configuration** tab for the hosts to which you are adding this new LUN, select **Storage** and run a **Rescan All...**
4. After the rescan is completed, click **Add Storage...**

5. Follow the process outlined in 4.5, “Storage connectivity” on page 42, but when prompted, select **Assign a New Signature** and click **Next**. See Figure 8-12.

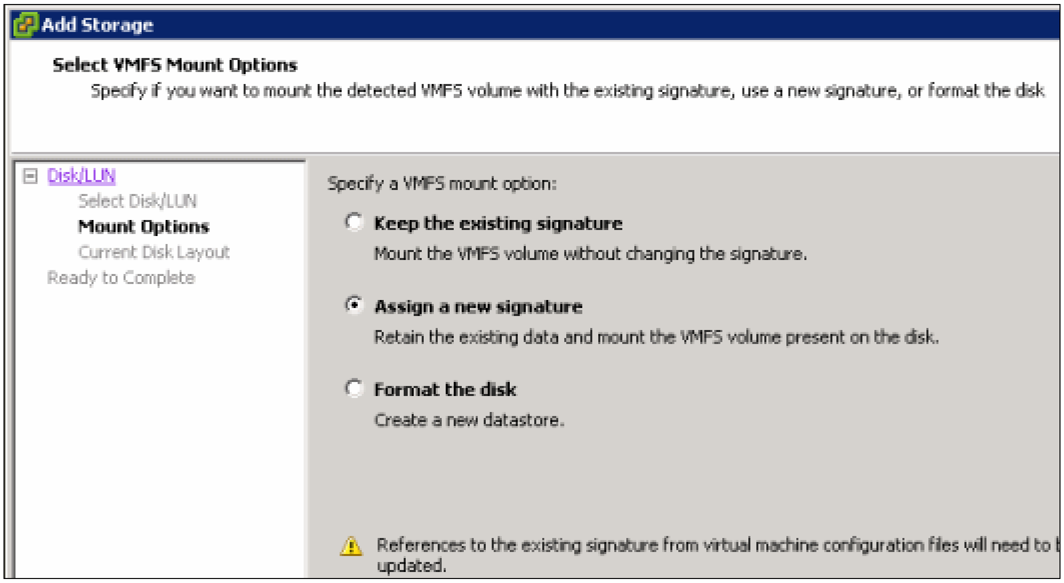



*Figure 8-12 Changing the LUN signature to avoid duplication*

## 8.4 Adding a virtual machine to the inventory

To add a virtual machine, follow these steps:

1. On the **Datastore** view, you see that the newly created VMFS datastore has the prefix `snap-xxxxxxxx-` and then the same name of the original datastore, as the same size, as shown in Figure 8-13.

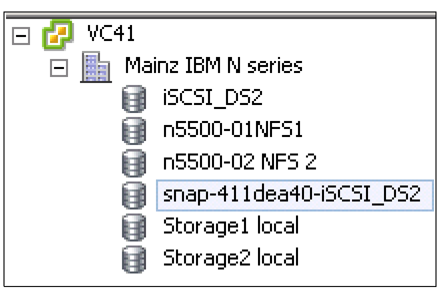



*Figure 8-13 New datastore name related to the cloned datastore*

2. Right-click the new datastore Figure 8-14, and select **Browse Datastore**. You can rename the datastore to something more logical if you prefer. In this example, for our purposes, we leave the automatically assigned name.

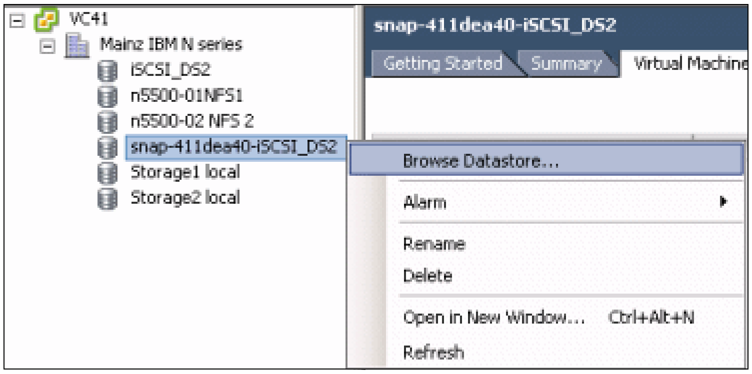



*Figure 8-14 Browsing the cloned datastore*

3. In the left pane of the Datastore Browser window (Figure 8-15), select one of the guests. In the right pane, right-click the **.vmx** file and select **Add to Inventory**.

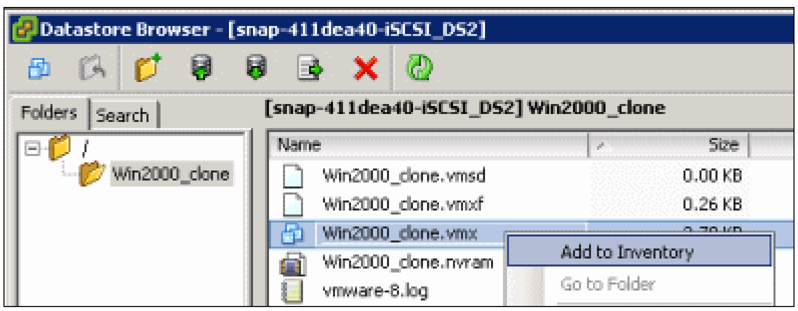



*Figure 8-15 Adding a Virtual Machine to inventory*

4. In the Add Inventory Wizard (Figure 8-16), provide a name for the new guest, select the inventory location, and click **Next**.

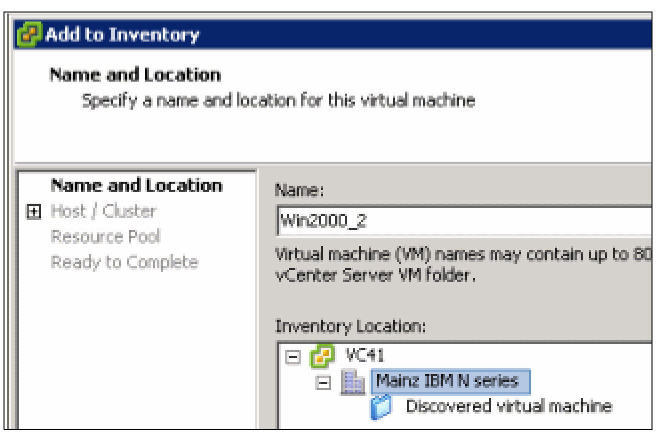



*Figure 8-16 Providing a name to the virtual machine being added*

5. In the Select the Host or Cluster panel (Figure 8-17), select a host or cluster. Click **Next**.

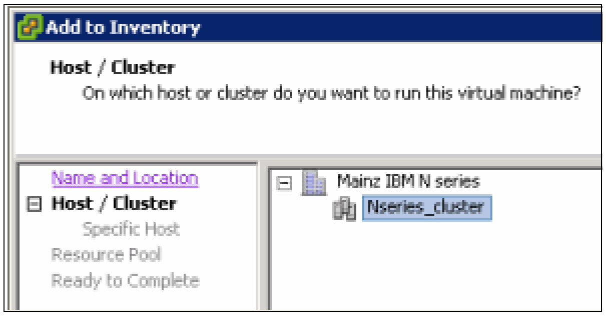



*Figure 8-17 Selecting a cluster*

6. In the Specify a Specific Host panel (Figure 8-18), select a specific host in a cluster that was selected. Click **Next**.

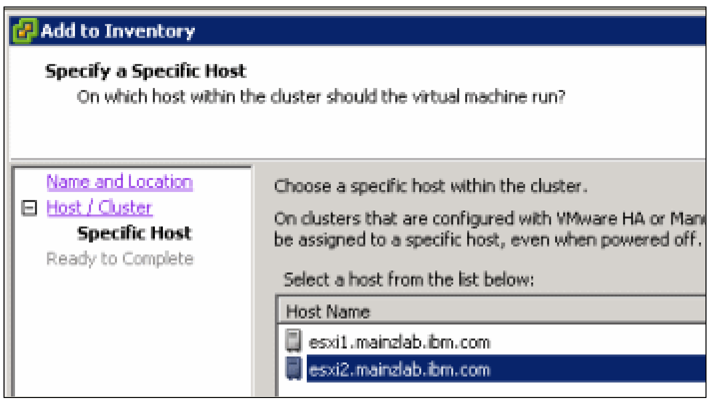



*Figure 8-18 Selecting a specific host*

7. To complete the addition of the guest to the host, confirm your choices and click **Finish**.

In our environment, we added the other guest, as shown in Figure 8-19.

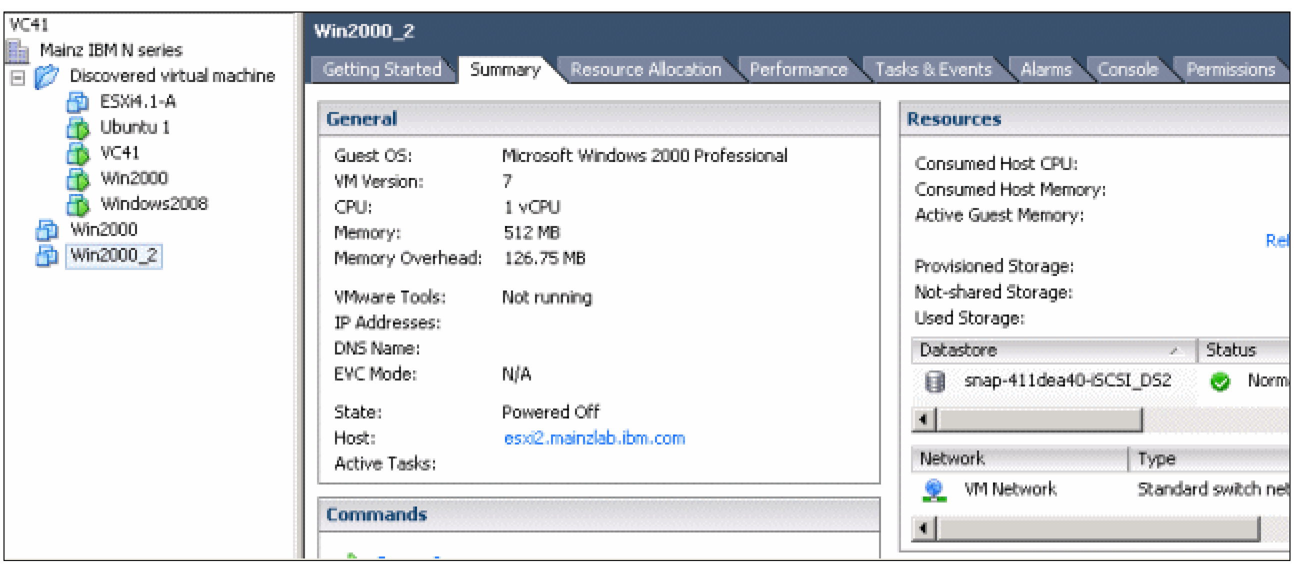



*Figure 8-19 Finished adding guests*

You are now finished with adding guests to the Inventory from a clone. As a final step, you might want to run A-SIS to deduplicate the blocks for all of these guests down to a single set. For more information, see Chapter 13, “Deduplication with VMware vSphere 4.1” on page 235.

## 8.5 Cloning VMware ESXi servers

Although installing VMware ESXi server from a CD is fairly quick and simple, you might want to deploy multiple servers in a short time. Deploying these servers from a cloned golden image is quicker and easier than using the CD.

To use an existing VMware ESX Server, quickly make it a golden image, and then return it to service, follow these steps:

1. In the vCenter, select the host that you want to use to make the golden image.
2. Remove the IP configuration of the host:
   a. Log in to the ESXi host console with the root user.
   b. Go to **Configure Management Network**
   c. Select **IP Configuration**
   d. Change the configuration to DHCP, as in Figure 8-20, and press **OK**.

      Here we are changing the server to be the image to DHCP, so the clones generated from it will not conflict when starting.

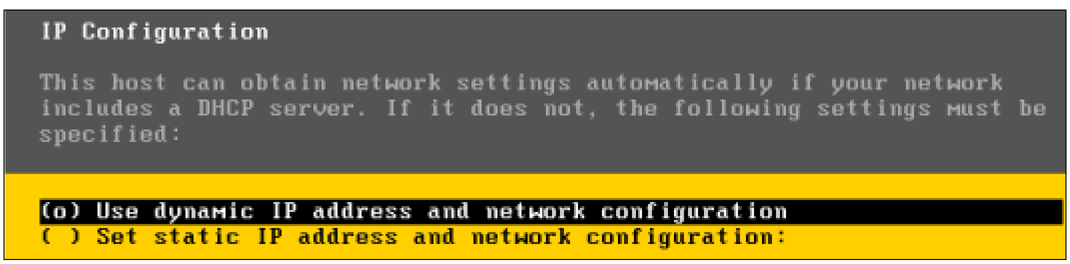



*Figure 8-20 Changing server to be the image to DHCP, so clones do not conflict when starting*

   e. Press Esc to exit this panel and Y to accept the management agents restart.
3. Shut down the host so the image is consistent.

4. On the N series system, take a Snapshot of the volume that contains the LUN that you want to clone, as in Figure 8-21.

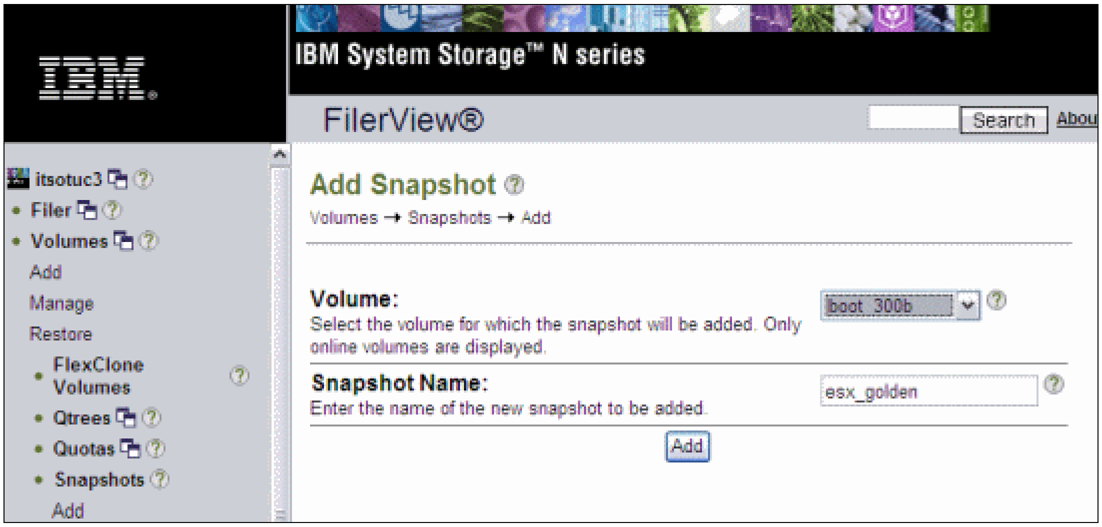



*Figure 8-21 Taking a Snapshot for the golden image*

5. Create a LUN clone by using the CLI of the N series system as Example 8-1.

*Example 8-1 Creating a LUN clone*

```
itsotuc3> lun clone create /vol/boot_300b/300c -b /vol/boot_300b/gold esx_golden
```

6. To separate the golden image from the parent LUN, split the clone as shown in Example 8-2.

*Example 8-2 Splitting the LUN clone*

```
itsotuc3> lun clone split start /vol/boot_300b/gold
Thu May  1 07:59:38 MST [itsotuc3: lun.clone.split.started:info]: Clone split wa
s started on LUN /vol/boot_300b/gold.
Thu May  1 08:03:01 MST [itsotuc3: lun.clone.split.completed:info]: Clone split
was completed on LUN /vol/boot_300b/gold.
```

Put the original host back in service by undoing the modifications that you made.

Now that you have a stand-alone golden image, continue as though it were days or months later and you now want to deploy a new VMware ESXi server:

1. Take a Snapshot of the volume where the golden image resides. Create a clone for use as a new host. Then split the new host's LUN from the parent, as shown in Example 8-3.

*Example 8-3 Making a new host LUN*

```
itsotuc3> snap create -V boot_300b get_golden
itsotuc3> lun clone create /vol/boot_300b/300c -b /vol/boot_300b/gold get_golden
Thu May  1 09:15:07 MST [itsotuc3: lun.clone.created:info]: Created Clone /vol/b
oot_300b/300c of LUN /vol/boot_300b/.snapshot/get_golden/300b
itsotuc3> lun clone split start /vol/boot_300b/300c
Thu May  1 09:16:07 MST [itsotuc3: lun.clone.split.started:info]: Clone split wa
s started on LUN /vol/boot_300b/300c.
itsotuc3> Thu May  1 09:21:26 MST [itsotuc3: lun.clone.split.completed:info]: Cl
one split was completed on LUN /vol/boot_300b/300c.
```

2. Map the LUN to the new host (300c):
   a. In the Manage LUNs pane of the FilerView panel (Figure 8-22), click the **No Maps** link for LUN 300c.

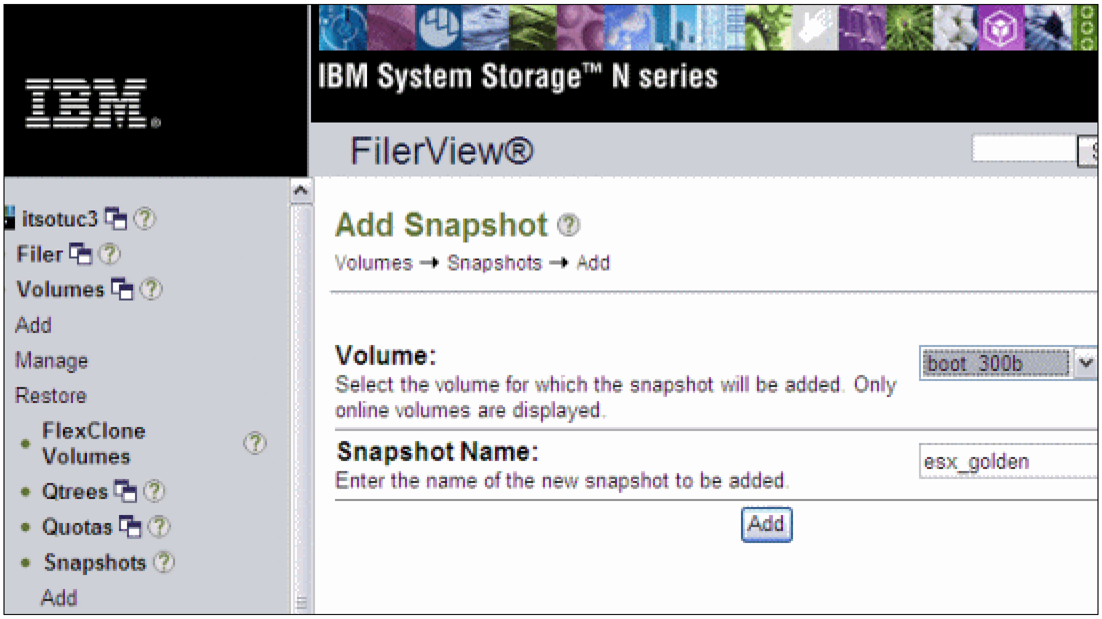



*Figure 8-22 Manage LUNs pane*

   b. In the LUN Map pane (Figure 8-23), select the **Add Groups to Map** link.

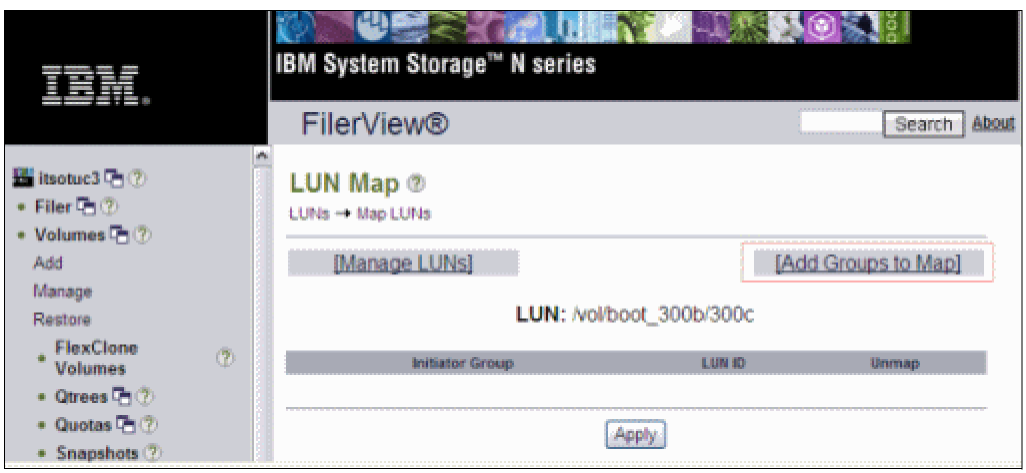



*Figure 8-23 LUN Map pane*

c. In the LUN Map Add Groups pane (Figure 8-24), select the host to which this LUN is to be mapped, and then click **Add**.

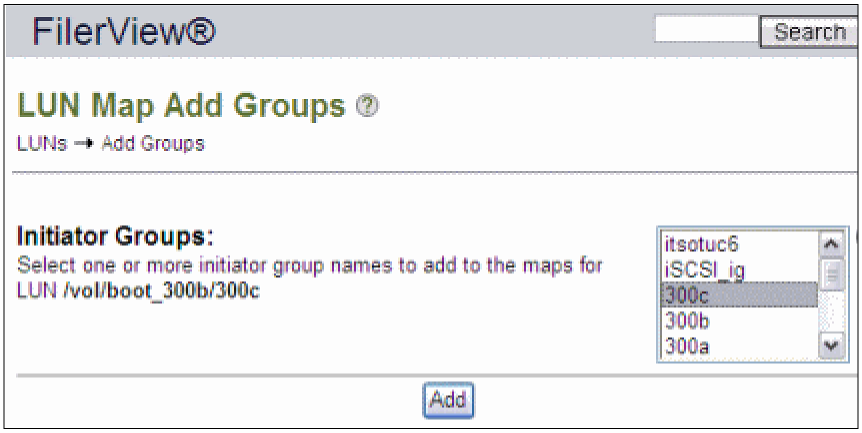



*Figure 8-24 LUN Map Add Group pane*

d. In the LUN Map pane (Figure 8-25), assign a LUN ID for this LUN that presents it to the host. For this boot LUN, for LUN ID, type 0, or the VMware ESXi server will not boot from it. Then click **Apply**.

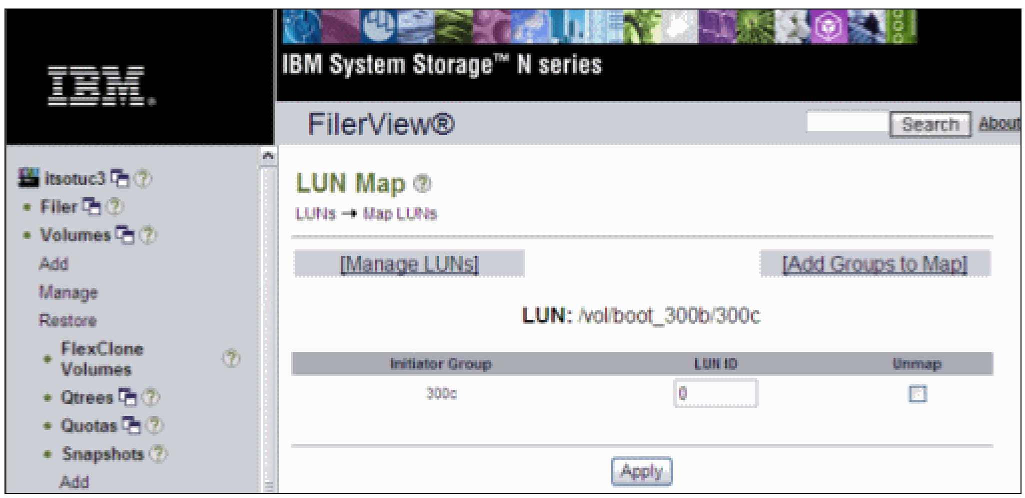



*Figure 8-25 LUN ID assignment*

3. After applying the LUN ID to the map, under LUNs in the left pane of the FilerView panel, click **Manage**. You now see your new LUN mapped to the new host, as shown in Figure 8-26. Notice that the LUN ID on which the LUN is mapped is 0.

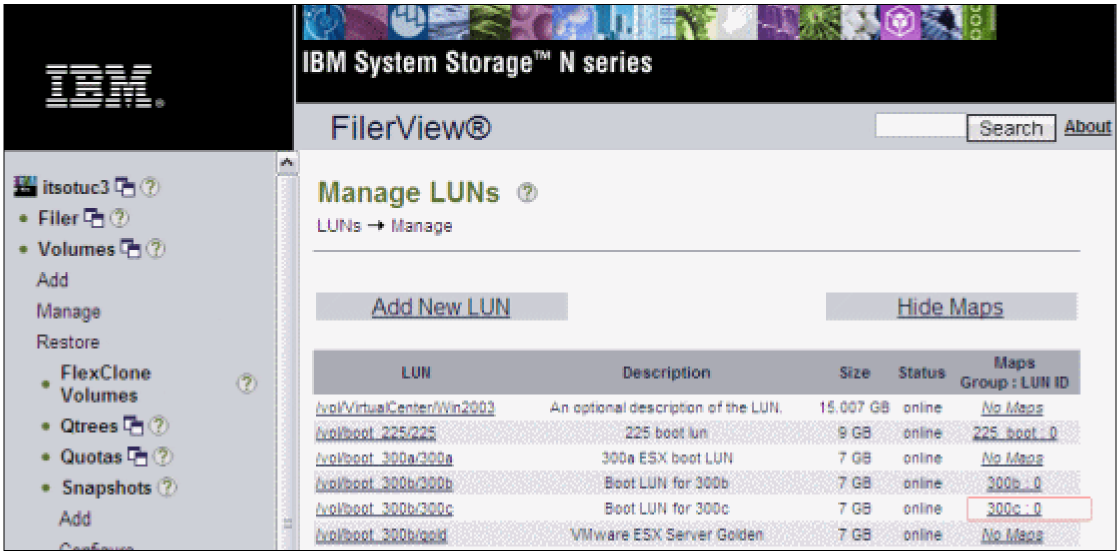



*Figure 8-26 Mapped LUN of the new host*

You have finished creating the LUN for the new host from the N series side. After the new host boots off the cloned LUN, configure the ESXi as shown in 5.4, “Installing the ESXi operating system” on page 86.

**Important:** To clone servers, you must ensure that they have the same hardware.

# 9

# Configuring snapshots

You need to plan the backup and recovery of your VMware environment carefully, depending on your requirements. You might be backing up data for various reasons, with each backup requiring a different strategy. In this chapter, we offer ways to help you accomplish this goal.

This chapter includes the following topics:

- Storage considerations
- Taking a snapshot
- Scheduling snapshots

## 9.1 Storage considerations

A snapshot is a point-in-time copy from data, which allows the administrators to recover the data in that specific point.

That technique is useful with virtual machines, because it provides the ability to recover a server to a specific point whenever needed. If a risky change is going to take place on a certain server, a snapshot can be taken just before the change begins. If anything goes wrong during the implementation, it is not necessary to follow the traditional restore approach of servers. That is, you do not need to install the operating system from scratch, install the backup, restore the software, and restore the data. The only step needed is to restore to a previous point in time. The server is up and running again in a matter of seconds or minutes, depending on the amount of data to be reverted.

Formerly, it was considered a best practice to separate the real server‘s data from transient data, such as temporary files and swapping partitions. But as virtualization implementations became more mature, this practice changed. Data separation does not add enough benefits to justify its implementation, because it changes the way the servers are configured.

The major benefit of data separation is reducing the amount of data to be stored on snapshots and replicated to remote locations in case of disaster recovery (DR) implementations.

However, keeping all the pagefiles in a single location creates a single point of failure, because if it fails, all the virtual machines are affected. The separation also adds an administrative burden. It requires the reconfiguration of all servers to point to a new disk in a new “transient datastore,” responsible to hold that temporary data.

For all these reasons, the new best practice is to keep the transient data stored with the server‘s data, providing a centralized management of the entire solution.

## 9.2 Using VMware snapshots

Snapshots are a valuable tool to manage the environment. Might they be used instead of a backup and restore solution? To understand this idea, you need to understand how snapshots work in the VMware world. Basically, the VMware snapshot system locks the virtual disks (.vmdk) at the moment of the snapshot.

All new information from that point in time is not written to the .vmdk, but to a file created on the same directory as the .vmdk. If the virtual disk is named C.vmdk, a file named C-000001.vmdk is created, and all new information is written on it stead of the C.vmdk. For each read or write operation, it is necessary to go to two different files, the original and the -00000x.vmdk, to complete the operation. It can cause serious performance delays, especially on high disk I/O virtual machines.

Because all the new information is never committed into the .vmdk, the snapshot file grows indefinitely. It can take all the available space on the datastore where it resides, which can cause a crash of all VMs that share the same datastore.

Another reason to avoid that approach is that if you keep taking snapshots, you end up accessing a number of files to get the information you need. If only one of those files gets corrupted for any reason, you lose all the information stored on that .vmdk. You must then consider how you can restore the data.

The same reasoning applies to disaster recovery cases. If your datacenter is severely damaged and you lose all the information residing there, you have no other copy of your data.

## 9.3 Integrating VMware and N series snapshots as a solution

But if we use the VMware snapshots as part of the solution, then we do not have to run the VMs over the snapshot files all the time. Such a result would be really great!

That solution can be achieved by integrating the N series snapshots with the VMWare ones.

N series snapshot processing makes a copy of all the data at the moment it runs. Then it makes that copy separate from the actual running LUN, as a clone. After the LUN cloning, you can delete your VMWare snapshots, avoiding the risks described in the previous session.

**Important:** This solution does not replace the backup and restore procedures, but it does provide a means to speed the recovery of the environment. It can be used together with planned backup and recovery procedures.

The following sections show you how to implement that solution:

### 9.3.1 Taking a snapshot

To use snapshots as a solution, take a virtual machine snapshot, then take a snapshot from the volume where the LUN and its respective datastore. Then remove the virtual machine‘s snapshot.

#### Taking a virtual machine snapshot

Use vCenter to take snapshots, as shown in the following steps:

1. Using a Virtual Infrastructure Client, connect to your vCenter.
2. Right-click a virtual machine and select **Snapshot** → **Take Snapshot** (Figure 9-1).

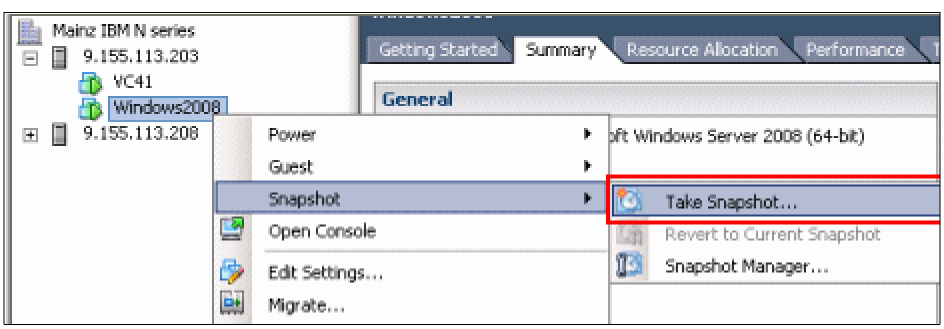



*Figure 9-1 Taking a snapshot of a virtual machine*

3. In the Take Virtual Machine Snapshot window (Figure 9-2), enter a name and description for the snapshot. If you select **Snapshot the virtual machine's memory**, the guest is suspended while the snapshot is taken. Selecting this option can affect any users who are connected to the guest at the time. Click **OK**.

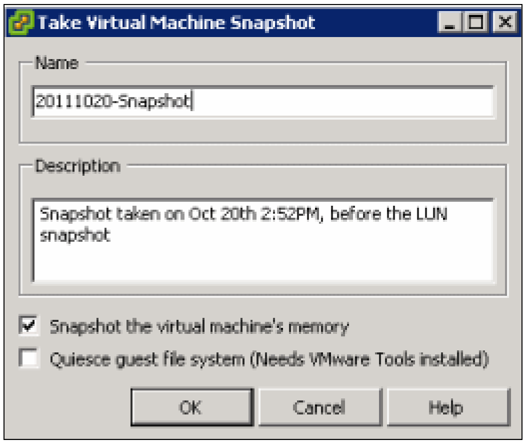



*Figure 9-2 VM Snapshot details*

4. Verify that the snapshot completed successfully, as in Figure 9-3.


*Figure 9-3 Guest snapshot complete*

## Taking a volume snapshot

After the snapshot is completed, take the N series snapshot. To take a snapshot of a volume where the LUN and its datastore reside, use FilerView, with the following steps:

1. In the left pane of the FilerView panel, select **Volumes** → **Snapshots** → **Add** (Figure 9-4).

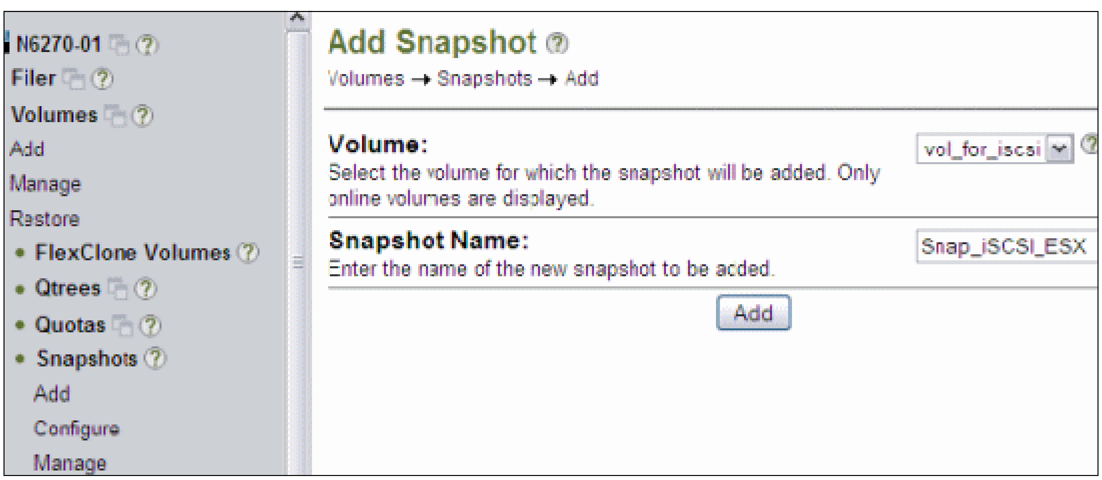



*Figure 9-4 Add Snapshot*

2. In the right pane, select the volume and provide a name for the snapshot. Click **Next**.
3. Figure 9-5 shows the success window that opens.

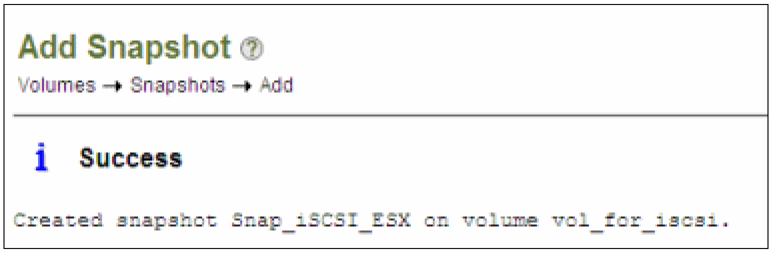



*Figure 9-5 Add Snapshot successful*

## Removing the virtual machine snapshot

1. Remove the VMware snapshot:

   a. In vCenter, right-click the guest and select **Snapshot** → **Snapshot Manager** as in Figure 9-6.

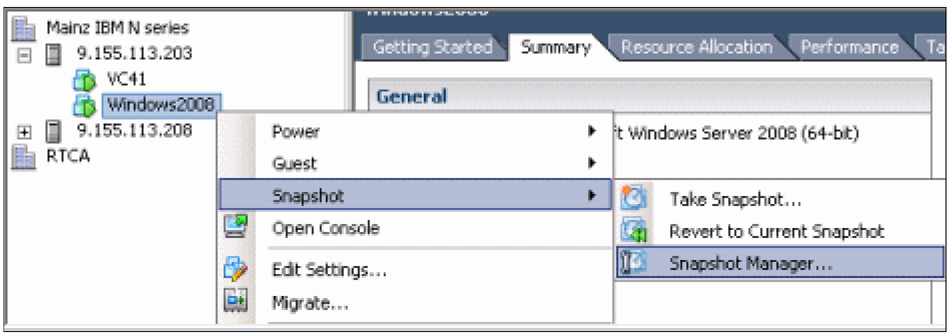



*Figure 9-6 Guest Snapshot Manager*

   b. In the Snapshots window (Figure 9-7), select the snapshot to delete, and click **Delete**.

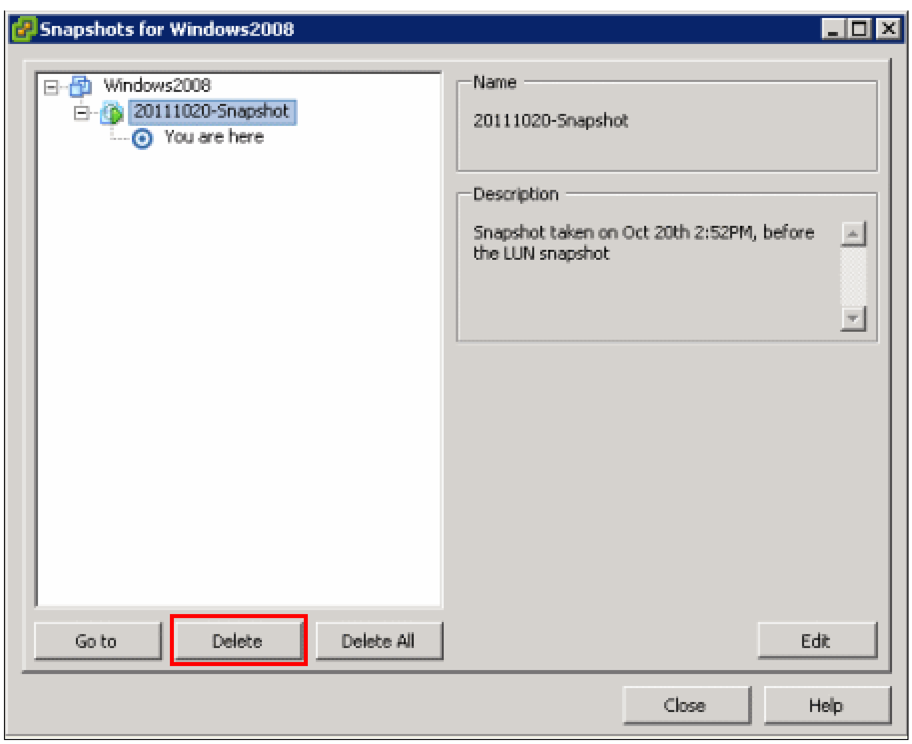



*Figure 9-7 Deleting a guest snapshot*

c. In the Confirm Delete window, click **Yes** to confirm the deletion.

d. In the Snapshot Manager window, in Figure 9-8, verify that the snapshot is no longer displayed.

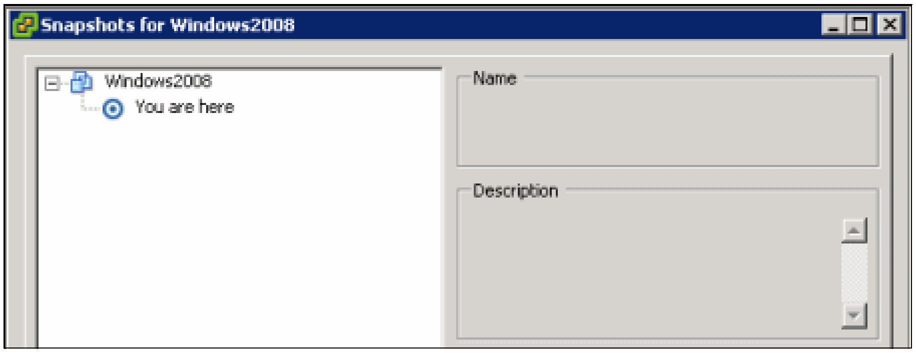



*Figure 9-8 Guest Snapshot deleted*

## 9.3.2 Scheduling snapshots

In a production environment, you can automate the snapshot process. vCenter can be used to schedule snapshots as follows:

1. Click **Home** → **Scheduled Tasks**, as in Figure 9-9.

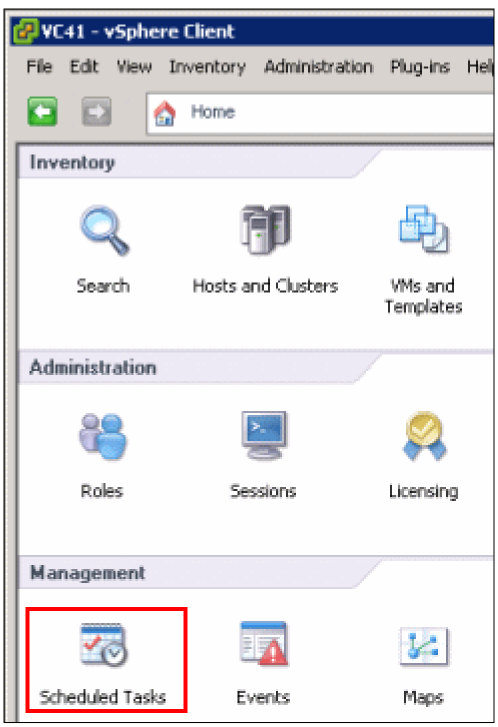



*Figure 9-9 Scheduled Tasks*

2. Click the **New** button in the left side top of the panel, as in Figure 9-10.


*Figure 9-10 Scheduling a new task*

3. Select the virtual machine and click **Next**.
4. Provide a name for the snapshot and select Memory Snapshot also, then click **Next**.
5. Provide a name, date, and time when the task will run, then click **Next**.
6. Enter your email address if you want the vCenter to inform you after the completion of that task, and click **Next**.
7. Review the scheduled task and click **Finish**.

The N series component can be scripted as indicated previously by using the **`snap create <vol-name> <snapshot-name>`** command, or it can be scheduled from FilerView.

Within FilerView, volume snapshot scheduling is configured automatically on all new volumes on the storage system. You must review the schedule for each new volume to ensure the best schedule settings.

To set the snapshot schedule for a volume, follow these steps:

1. In the left pane of the FilerView window, select **Volumes** → **Snapshots** → **Configure**. You will have a number of options as shown in Figure 9-11. It is important to set the number of snapshots to keep in accordance with your storage capacity. Also, schedule the snapshot to occur when the production utilization is low to avoid bottlenecks. Click **Apply**.

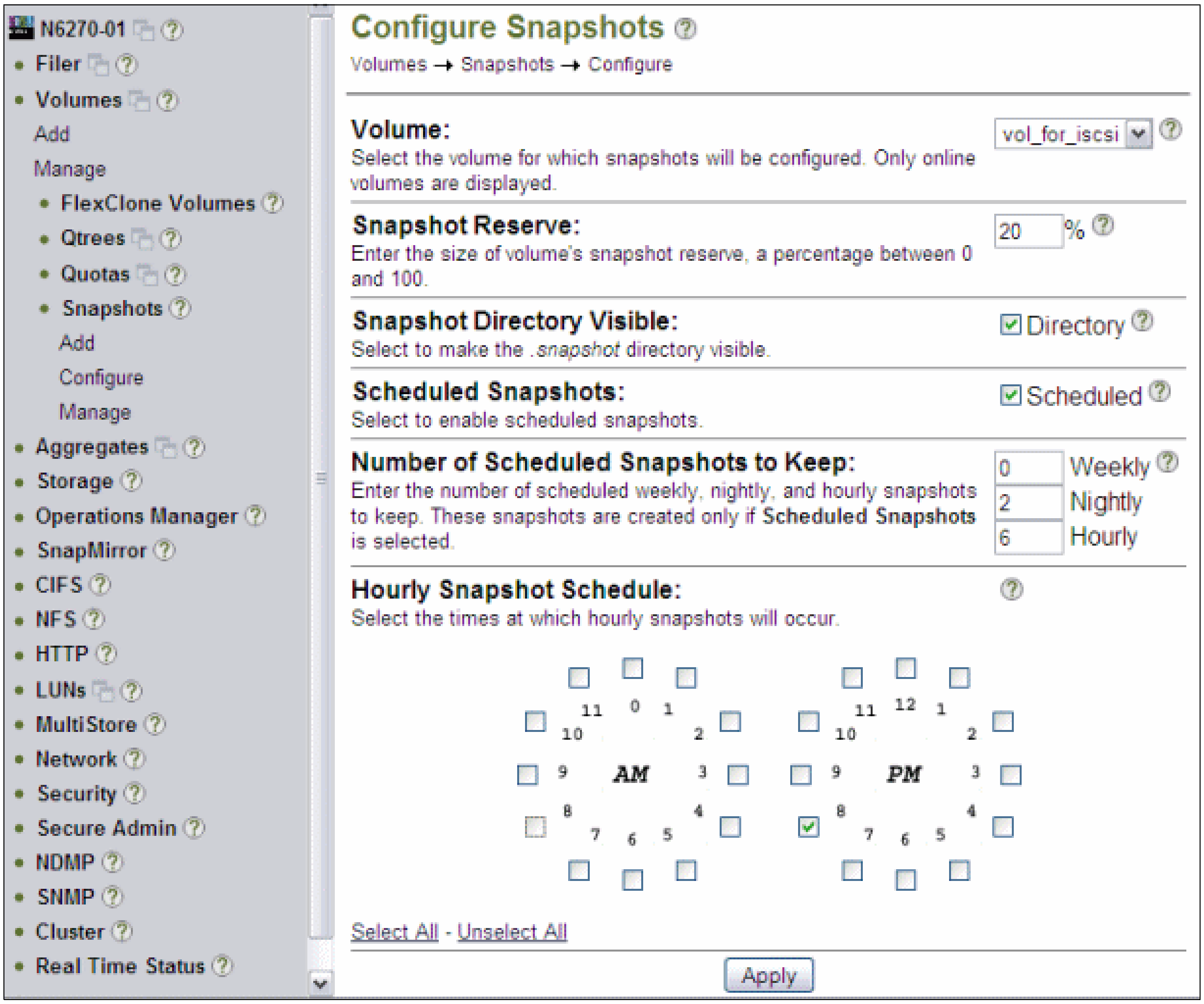



*Figure 9-11 Snapshot scheduling options*

2. Check if you got the Success message, indicating that your settings were implemented correctly, as shown in Figure 9-12.

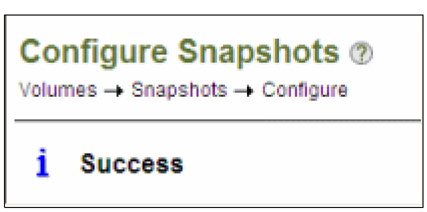



*Figure 9-12 Success creating the schedule*

# 10

# Recovery options

You need to plan the backup and recovery of your VMware environment carefully, depending on your requirements. The reason for recovery might require one of the following main strategies:

- Recovery from a failed or corrupted LUN or volume
- Recovery from a failed server (guest)
- Recovery from accidental deletion of user files

For information about recovery from a failed storage system, ESX server, or whole server environment, see Chapter 12, “High availability and disaster recovery” on page 215.

Recovery of a snapshot can be done at the volume or LUN level directly from the N series system. Files or guests can be recovered only by using a clone of a LUN that is mounted and that restores the required data.

This chapter includes the following topics:

- Restoring a volume
- Restoring data from a cloned volume, as with FlexClone
- Recovering an entire virtual machine
- Recovering files within a guest

## 10.1 Restoring a volume

Restoring volumes requires retrieving data from a snapshot, so you must have at least one in order to restore a volume. Snapshot creation and scheduling are covered in Chapter 9, “Configuring snapshots” on page 169.

Restoring a volume from a snapshot overwrites the existing volume with the backup version. You might want to perform this task where a volume was unintentionally deleted or corrupted.

To restore a volume, use the Data ONTAP FilerView tool as follows:

1. Select **Volumes** → **Restore** from the side menu, as in Figure 10-1.


*Figure 10-1 Volume restore*

2. In the Welcome pane of the Volume Restore Wizard, which guides you through the restoration process as in Figure 10-2, click **Next**.


*Figure 10-2 Volume Restore Wizard*

3. In the Volumes pane (Figure 10-3), select the volume that needs to be recovered. Click **Next**.

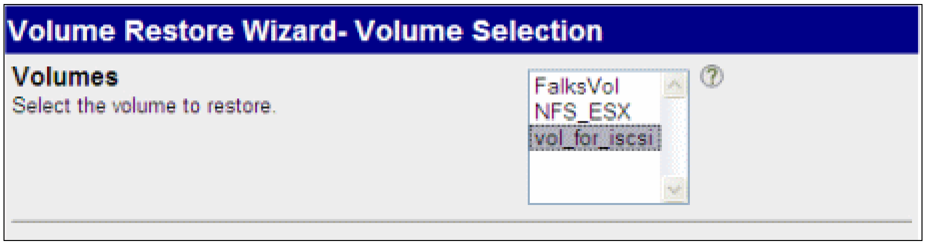



*Figure 10-3 Selecting the volume to restore*

4. In the Snapshots pane (Figure 10-4), select the snapshot that you want to restore. If you choose an old snapshot, all newer snapshots become unavailable for future restores. Click **Next**.

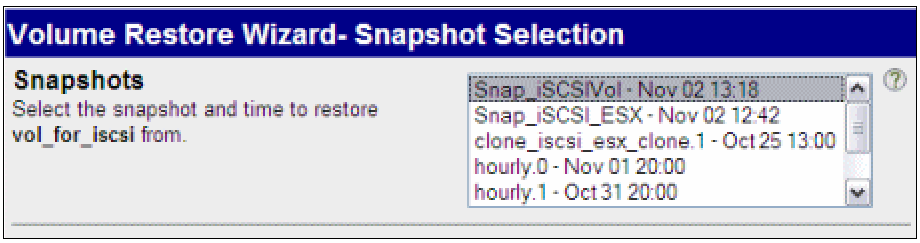



*Figure 10-4 Selecting the volume snapshot*

5. In the Commit pane (Figure 10-5), check the details of the restore that you requested, and click **Commit** if you want to do the restore.

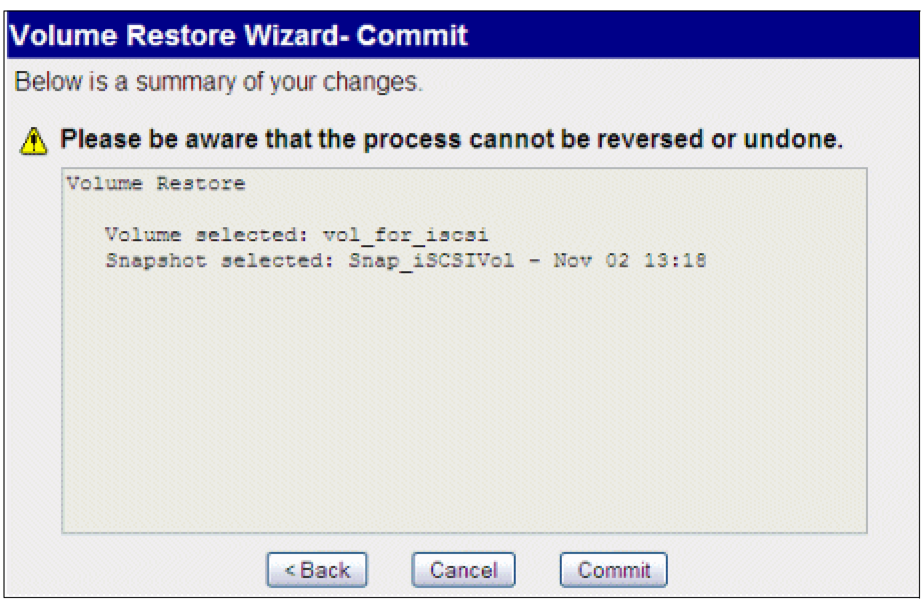



*Figure 10-5 Committing the volume restore*

6. In the Success pane (Figure 10-6), verify that the volume restore process completed successfully, and click **Close**.

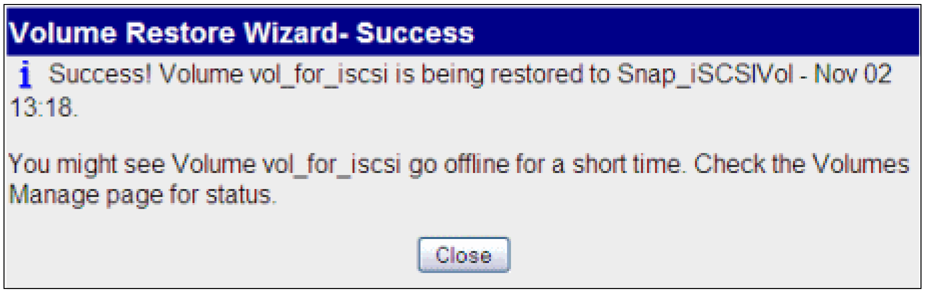



*Figure 10-6 Completing the volume restore*

# 10.2 Restoring data from a cloned volume, as with FlexClone

To restore a volume while keeping the existing volume intact, a clone of a snapshot backup is required. You do this process when only some of the data from a volume was lost or needs to be recovered.

> **Preferred practice:** Use the clone for a short time while data recovery is occurring, and then destroy it. Do not take snapshots while the clone exists, which can lead to contention.

## 10.2.1 Creating a clone

To create a clone, using FilerView, complete these steps:

1. In the left navigation pane of the FilerView window (Figure 10-7), select **Volumes** → **FlexClone** → **Create**.

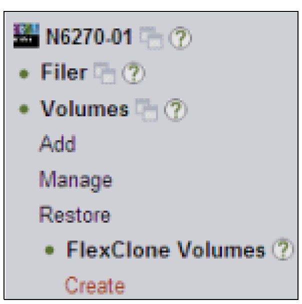



*Figure 10-7 Creating a FlexClone*

2. In the Welcome pane (Figure 10-8) of the FlexClone Wizard, which steps you through the cloning process, click **Next**.

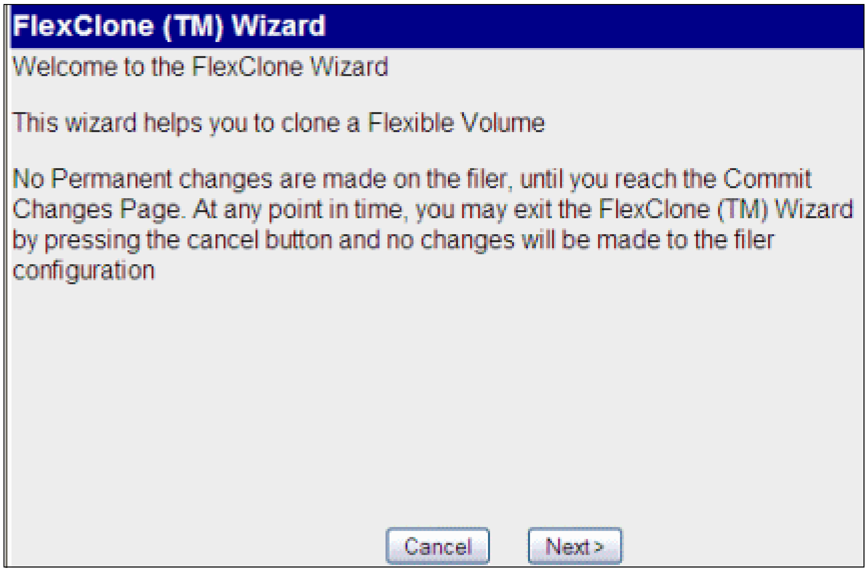



*Figure 10-8 FlexClone Wizard*

3. In the Clone a Flexible Volume pane (Figure 10-9), enter the name of the new clone. Select the volume to be cloned and the Space Guarantee option that you require. Click **Next**.

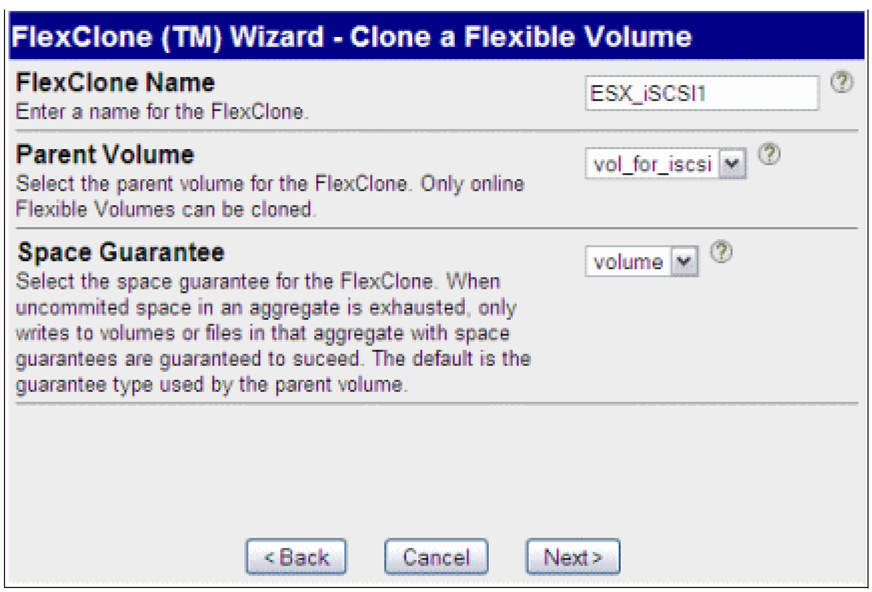



*Figure 10-9 FlexClone settings*

4. In the Parent Snapshot pane (Figure 10-10), select the snapshot of the volume that you want to clone. This step is not a destructive action like the volume restore. More recent snapshots are still available after the clone is complete. Click **Next**.


*Figure 10-10 Selecting the snapshot for FlexClone*

5. In the Commit pane (Figure 10-11), check the details of the FlexClone that you requested. Click **Commit** if you want to create the clone.

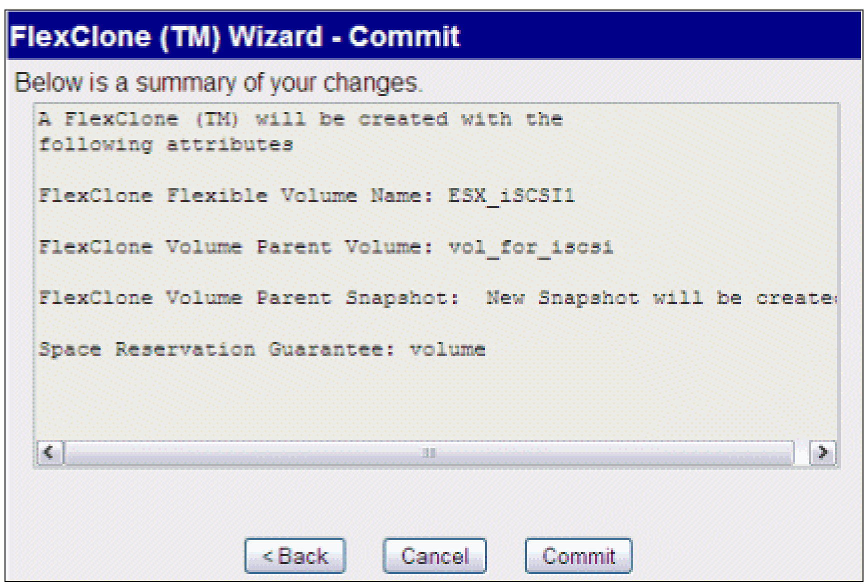



*Figure 10-11 Committing the FlexClone creation*

6. In the Success pane (Figure 10-12), verify that the FlexClone creation process completed successfully, and click **Close**.

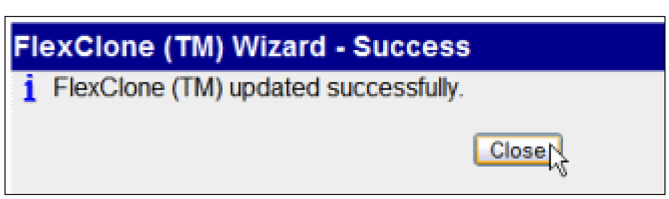



*Figure 10-12 FlexClone creation complete*

Now the clone is created, and all data (including LUNs) that was in the original volume, when the Snapshot was taken, is also there. Any LUNs, however, are not mapped, and therefore, cannot be mounted.

> **Alternative process:** This process uses the FlexClone feature in FilerView. Alternatively, you can use the following command on the N series command line:

```
lun clone create <clone_lunpath> [-o noreserve] -b <parent_lunpath>
<parent_snap>
```

## 10.2.2 Configuring the cloned LUN to be accessed

After the clone is created, you must bring online the LUNs (if any) that you want to access. Map the LUN to a host or hosts, then create a datastore over it.

### Mapping a LUN to hosts

1. In the FilerView window, in the left navigation pane, select **LUNs** → **Manage**, and you see the cloned LUN, as in Figure 10-13. It is offline and not mapped to any host, so we want to configure it.

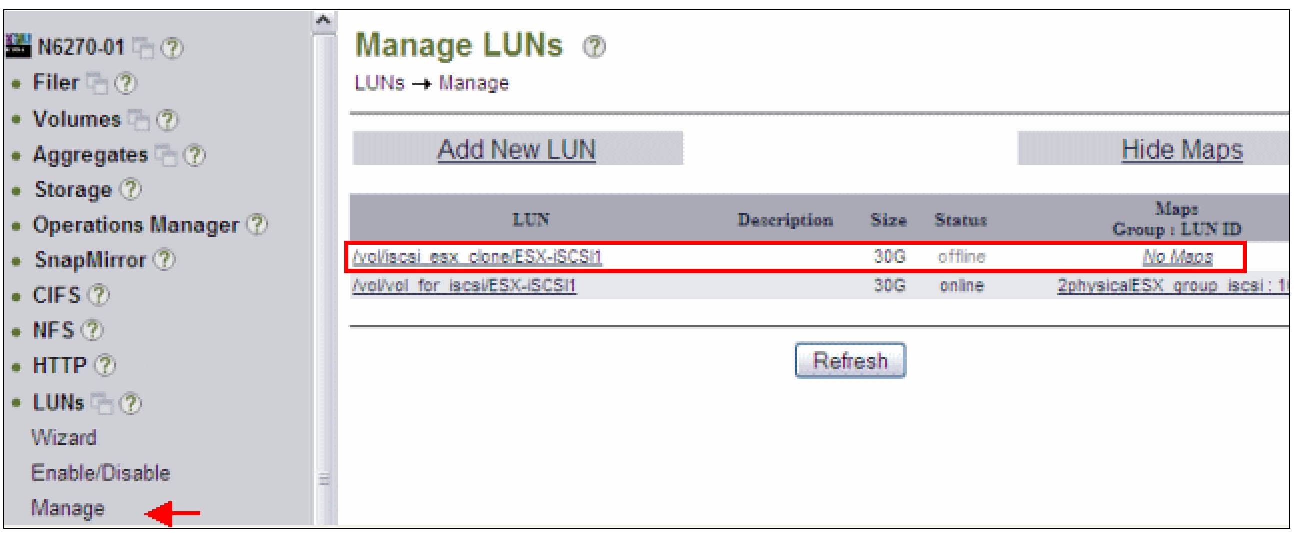



*Figure 10-13 The cloned LUN*

2. Click the LUN and then click **Online** to make it available, as in Figure 10-14.

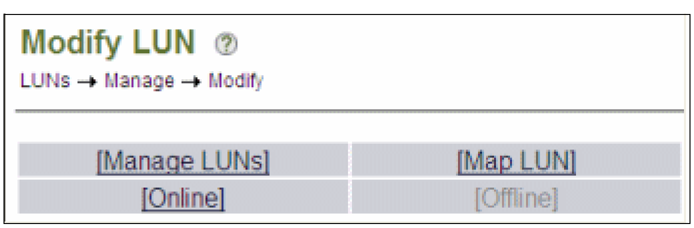



*Figure 10-14 Making the LUN Online*

3. Then click **LUNs** → **Manage** again and click **No Maps** on the cloned LUN. It opens a panel to select the Initiator Group, as in Figure 10-15. Click **Add Groups to Map**.

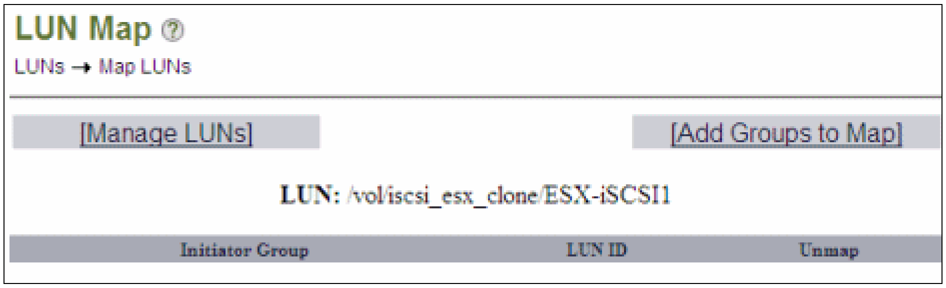



*Figure 10-15 Add Groups to Map*

4. Select the group and click **Add**, as in Figure 10-16.

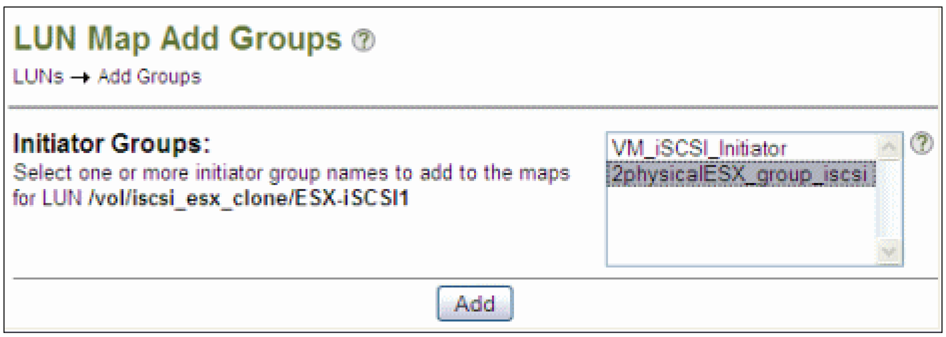



*Figure 10-16 Selecting Initiator Group*

5. Type a LUN ID for the cloned LUN and click **Apply**, as in Figure 10-17.

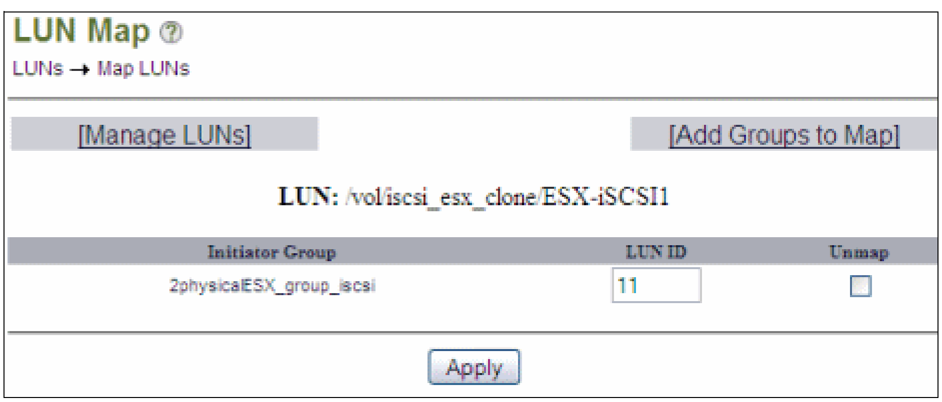



*Figure 10-17 LUN ID for the cloned LUN*

6. A Success message displays, as in Figure 10-18.

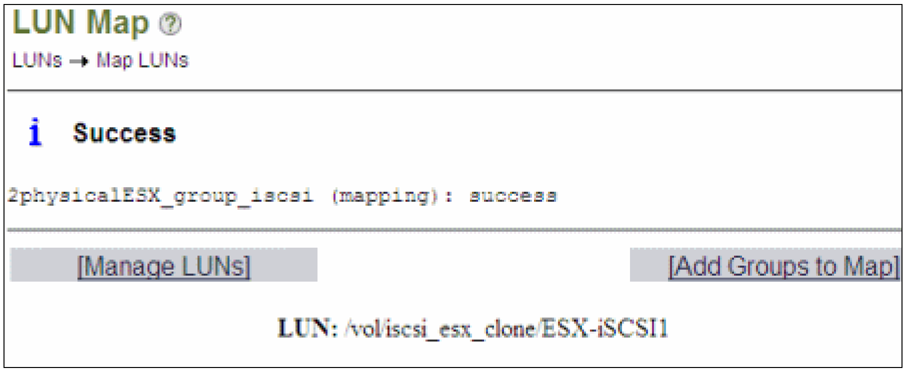



*Figure 10-18 Cloned LUN configuration completed on N series*

## Creating a datastore with the cloned LUN on VMware

Follow these steps:

1. On VMware side, select a host present on the initiator group and click **Rescan All**. Go to the Storage Adapters menu and select the iSCSI connection. You see the new LUN 11 available on the host, as shown in Figure 10-19.

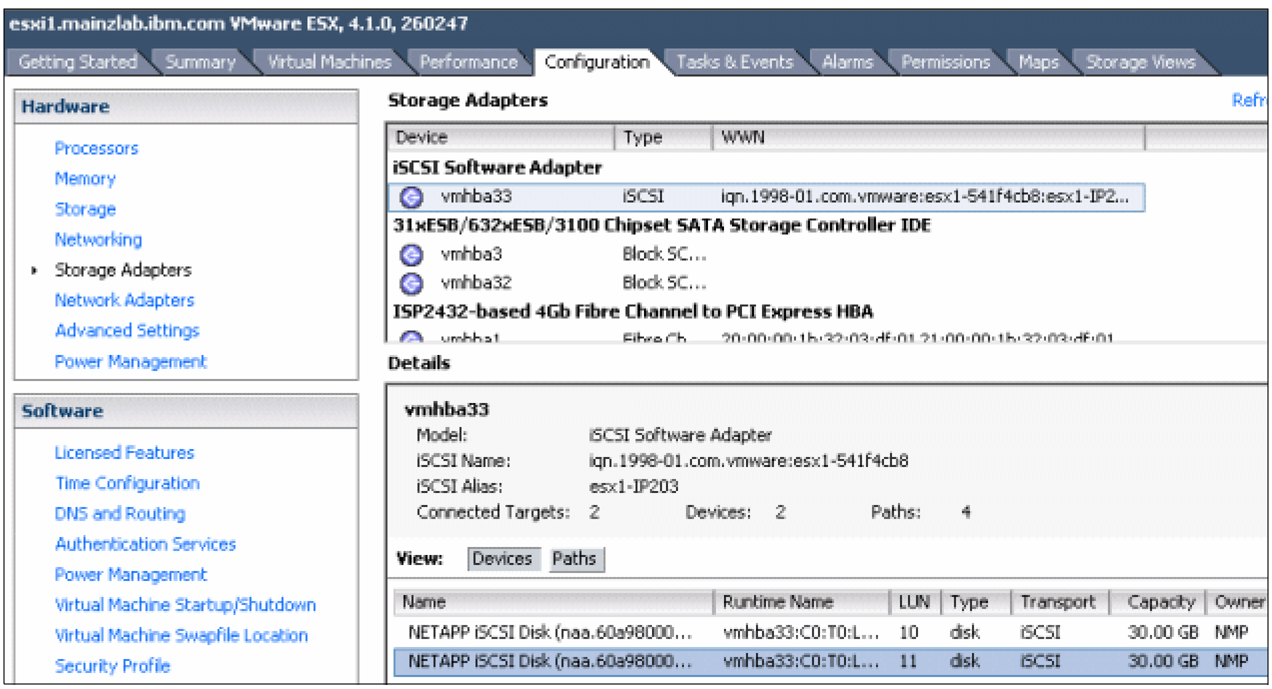



*Figure 10-19 The cloned volume shown with the LUN number defined on N series*

2. Click **Storage**, then click **Add Storage...**
3. On the Add Storage menu, select **Disk/LUN** and click **Next**.
4. The cloned LUN is available with the VMFS label as the name of the datastore from which the LUN was cloned. Select the cloned LUN and click **Next**.
5. In the Mount Options panel, change the radio button to **Assign a new signature**, as shown in Figure 10-20. That option enables the copy from the cloned datastore into the existing one.

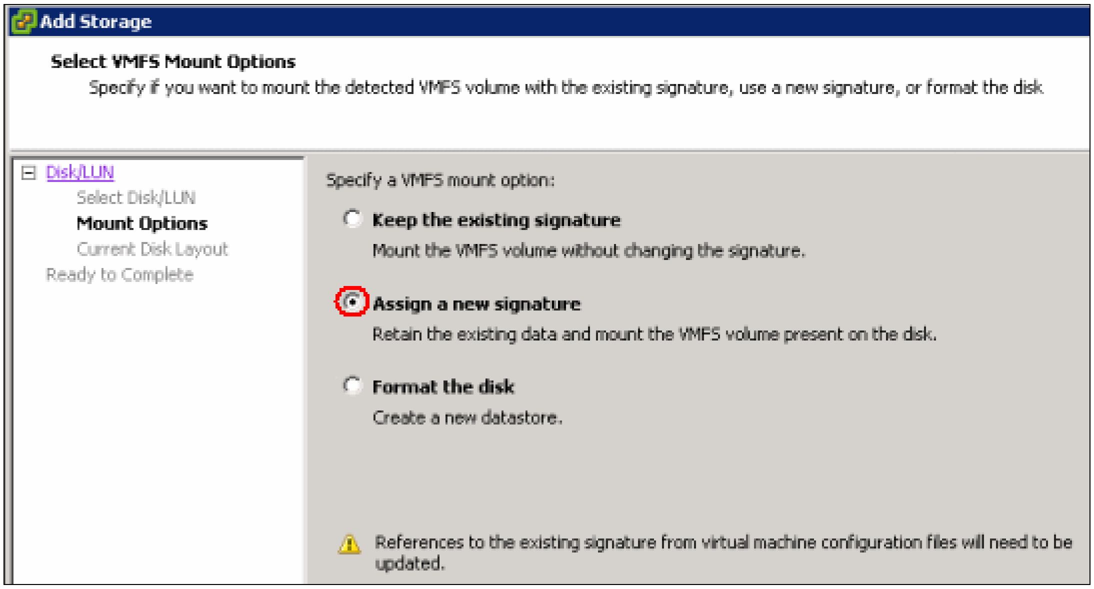



*Figure 10-20 Changing to Assign a new signature*

6. Review the information shown on the Current Disk Partition and click **Next**.
7. In the Ready to Complete panel, observe that a new signature is going to be applied to the LUN, as in Figure 10-21. Click **Finish**.

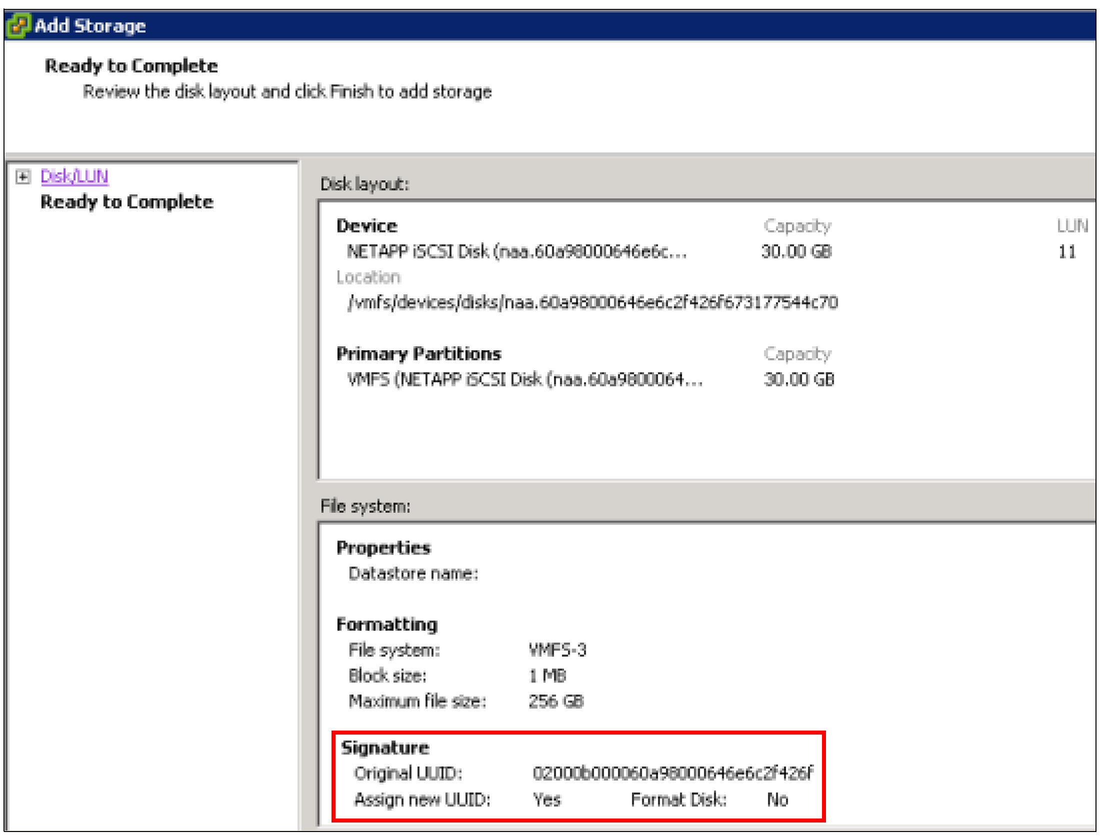



*Figure 10-21 A new signature is applied to the LUN*

8. After adding the datastore, it will have a name referencing the cloned LUN/datastore, as shown in Figure 10-22.

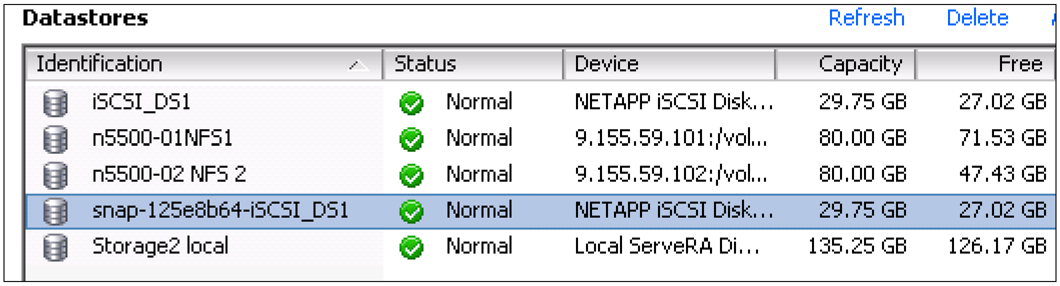



*Figure 10-22 The cloned LUN creates a datastore referring the original one*

# 10.3 Recovering an entire virtual machine

To recover a guest because of data corruption, the original guest files are replaced with the files of the cloned guest created in the previous sections.

## 10.3.1 Copying data into the original guest datastore

If you are restoring all of the virtual machines, then they probably have a problem and are down. If they are still running, make sure to turn them off before copying data over them.

To recover an entire virtual machine, follow these steps:

1. Browse the guest datastore, as in Figure 10-23.

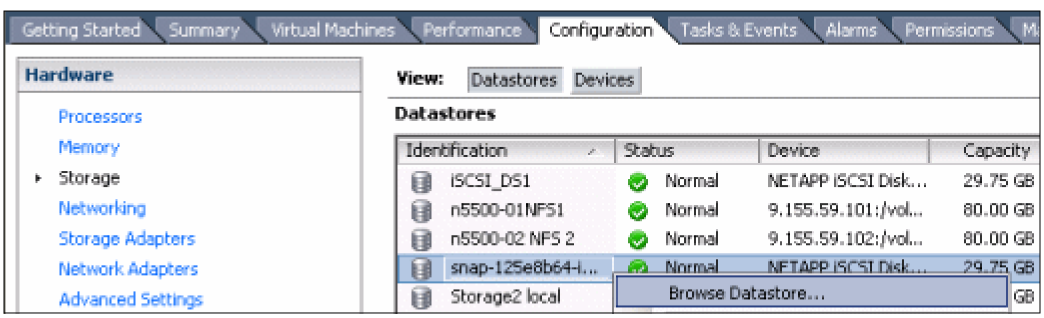



*Figure 10-23 Browsing the datastore from where data is to be copied*

2. Browse to the folder of the virtual machine to be recovered. Select all the files, right-click them, and click **Copy**, as in Figure 10-24.

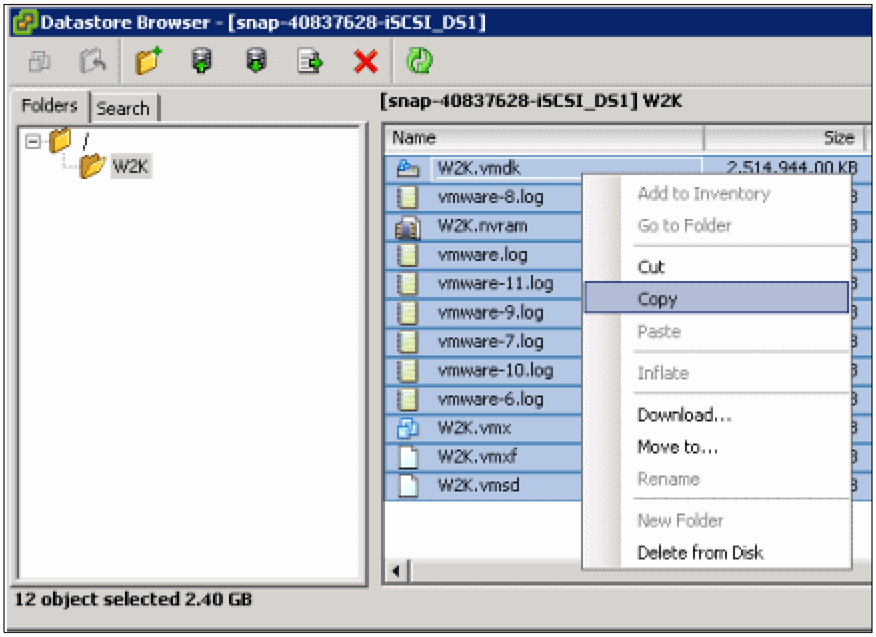



*Figure 10-24   Copying the files from the cloned datastore*

3. Browse to the original datastore, go to the virtual machine to be restored, right-click a blank area, and select **Paste**, as in Figure 10-25.

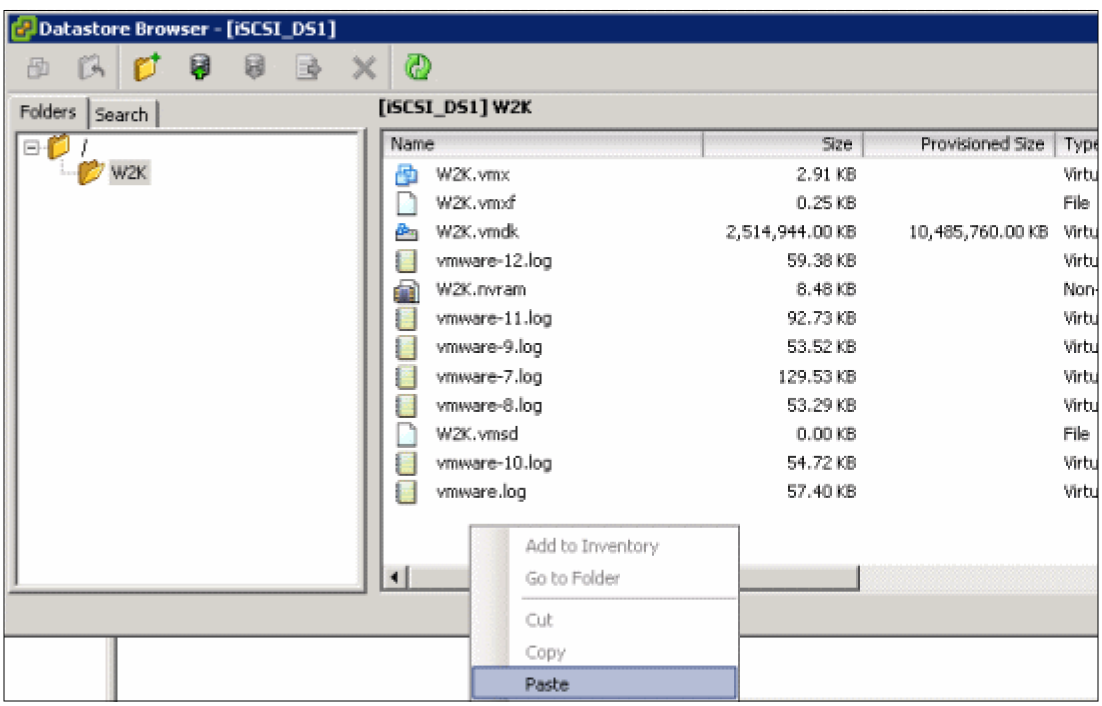



*Figure 10-25   Pasting the VM files over the original datastore / VM folder*

4. Click all **Yes** boxes to confirm the overwriting of its data.

5. Observe the progress of the copies on the Recent Tasks tab, as in Figure 10-26.

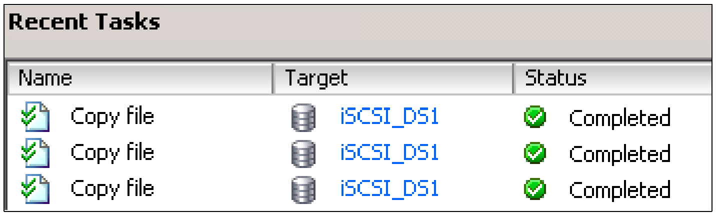



*Figure 10-26 The copy data completion status on Recent Tasks tab*

6. At the end of the data moving, start the virtual machine if you want.
7. If the cloned LUN/datastore contains a snapshot, use Snapshot Manager to delete it, which commits the data from the delta disks into the original virtual disk.

## 10.3.2 Recovering the RDM from Snapshot copy

Recovering the Raw Device Mapping (RDM) from a Snapshot is quick and easy. You shut down the VM, replace the LUN, and start the VM again, as explained in the following steps:

1. Open vCenter.
2. Select the guest you want and power it off.
3. Connect to the N series system console through SSH, telnet, or a console connection.
4. Clone the original LUN from a recent Snapshot copy:
   ```
   lun clone create <clone LUN path> –b <original LUN path> <Snapshot name>
   ```
5. Take the current version of the LUN in use offline:
   ```
   lun offline <LUN path>
   ```
6. Bring the cloned LUN online:
   ```
   lun online <LUN path>
   ```
7. Map the cloned LUN:
   ```
   lun map <LUN path> <igroup> <ID>
   ```
8. Back on vCenter, select the virtual machine you changed and power it on.
9. Validate that the restore is to the correct version. Log in to the virtual machine, and verify that the system was restored to the proper point in time.
10. Connect to the N series system console through SSH, telnet, or a console connection.
11. Delete the original LUN:
   ```
   lun destroy –f <original LUN path>
   ```
12. Split the clone into a whole LUN:
   ```
   lun clone split start <cloned LUN path>
   ```
13. Optional: Rename the cloned LUN to the name of the original LUN:
   ```
   lun mv <cloned LUN path> <original LUN path>
   ```

### 10.3.3 Recovering virtual machines from an NFS Snapshot copy

NFS provides a quick method to recover a guest from a Snapshot copy.

In summary, the process described next powers off the guest, restores the virtual disk (.vmdk), and powers on the guest. To complete this process, follow these steps:

1. Open vCenter.
2. Select the d virtual machine you want and power it off.
3. Browse the datastore where the .vmdk are located and go to the folder containing those files.
4. Rename the .vmdk, so a new file can be created when recovered from N series Snapshot.
5. Connect to the N series system console through SSH, telnet, or a console connection.
6. Restore the VMDK file from a recent Snapshot copy:

   ```
   snap restore –t file -s <snapshot-name> <original VMDK path> <original VMDK
   path>
   ```

7. Return to vCenter, select the virtual machine, and start it.
8. Validate that the restore is to the correct version. Log in to the guest, and verify that the system was restored to the proper point in time.
9. Delete the renamed .vmdk files from the datastore, browsing it.

## 10.4 Recovering files within a guest

Rather than recovering a whole guest from backup, sometimes only a few files need to be recovered within the guest. You can recover those files directly if the guest has backup client software installed and is sending backups to a central backup server. But if the only backup available is the entire LUN, an alternative method must be used.

If snapshots are implemented, files can be recovered from a cloned snapshot with no additional backup infrastructure required. Because the files are encapsulated within the guest .vmdk file, the file must be mounted by a virtual machine on the target server or another virtual machine.

> **Tip:** Using the target guest to mount the cloned .vmdk file is the most straightforward method. However, unmounting the file requires an outage on the guest. Therefore, plan for its use on a production guest. This example uses a temporary VM created for this task that can be removed after the recovery is complete, or kept for future file recoveries.

## 10.4.1 Creating a temporary recovery guest

You can create a temporary guest from a template or installing the operating system (OS) from a media. The temporary virtual machine must be compatible with the original OS.

## 10.4.2 Connecting the cloned virtual disk to the temporary guest

After the guest is created (our VM is named Temp-VM), connect it to the cloned guest disk:

1. Right-click the temporary guest and select **Edit Settings**
2. In the Virtual Machine Properties window, on the **Hardware** tab, click **Add** as in Figure 10-27.

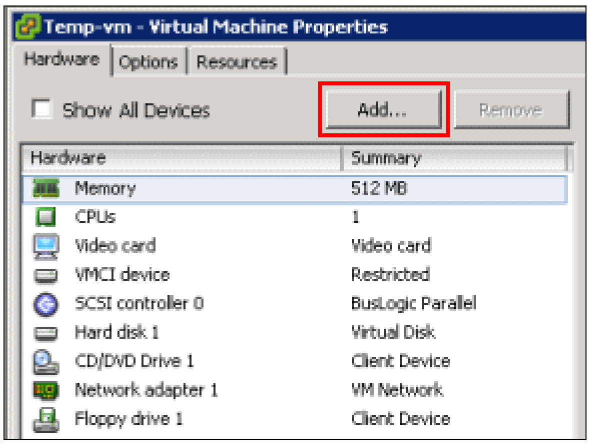



*Figure 10-27 Adding disk to the temporary VM*

3. Select **Hard Disk** and click **Next**.
4. Select "Using an existing virtual disk" as shown in Figure 10-28, and click **Next**.

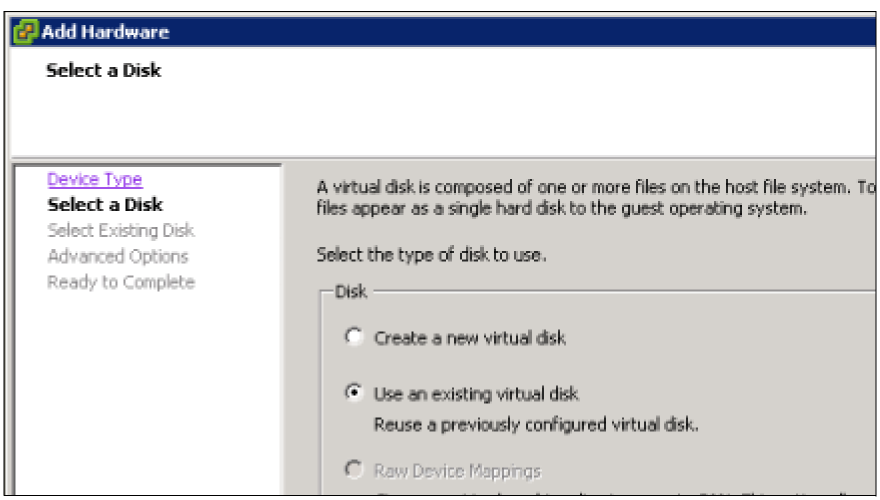



*Figure 10-28 Adding an existing disk*

5. On Select Existing Disk, browse to the datastore mounted over the recovered LUN. Find the disk from where the data is to be copied, as shown in Figure 10-29, then click **Next**.

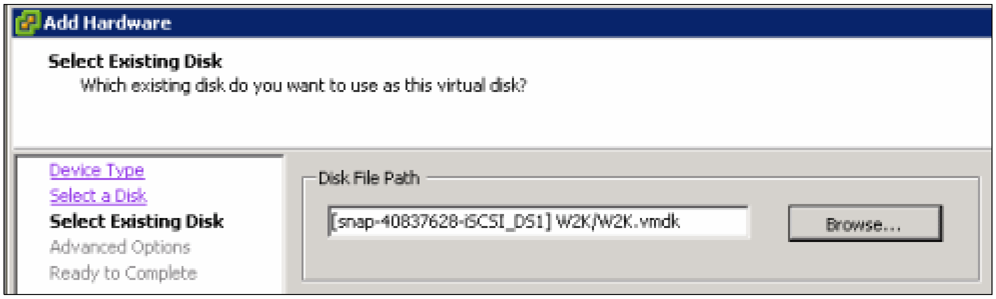



*Figure 10-29 Browse recovery datastore until finding the .vmdk containing the data wanted*

6. On the next panel, Advanced Options, accept the default SCSI controller being assigned to the disk and click **Next**.
7. On the Ready to Complete panel, review the entered information and click **Finish**.
8. Check the Recent Tasks list for successful reconfiguration of the guest (Figure 10-30).

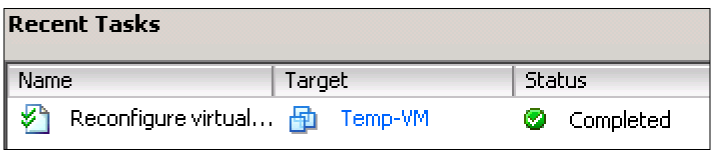



*Figure 10-30 Completion of the adding disk task*

## 10.4.3 Copying the files to the target guest

The temporary guest is now ready to be started in order to provide the data back to the original virtual machine. We now actually copy the data from one to another, as shown in the following steps:

1. Right-click the temporary guest, select **Power** and then **Power On**.
2. To access the guest, log on to the console. Right-click it and select **Open Console**.
3. After the OS comes up, log to it and set an IP, so it can share data with the original virtual machine. You might get a warning saying that the OS completed the installation of a new device (the added disk), requesting a restart. As a restart is not necessary, click **No**.

4. Notice how the guest has a second local disk, which is E: in this case. This disk is the cloned disk from where the data is to be recovered (Figure 10-31).

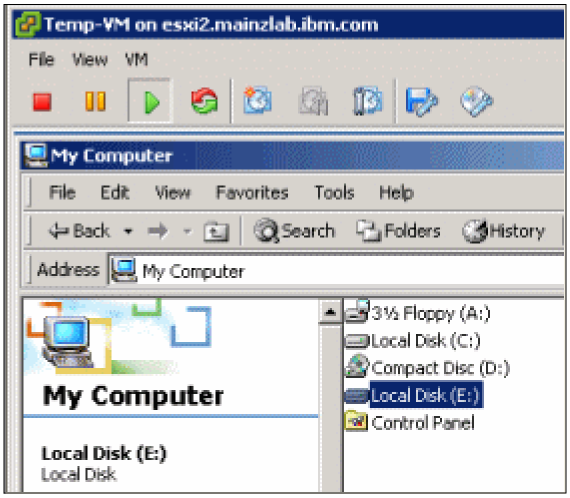



*Figure 10-31 The disk from which the data is to be recovered*

5. Map a network drive pointing to the original virtual machine (in this case, Prod-VM) and the disk to receive the restored data (Figure 10-32).

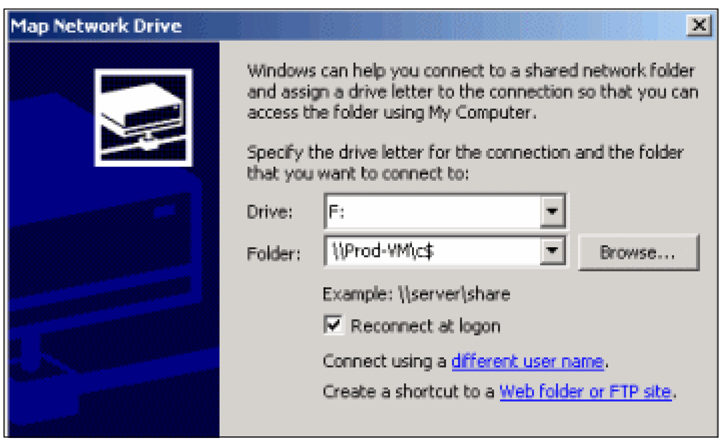



*Figure 10-32 Mapping the destination drive on the original virtual machine*

6. Copy the data from your restored VM into the mapped drive.

## 10.4.4 Disconnecting the cloned disk from the temporary guest

After file recovery is completed, shut down the temporary guest, so that the cloned disk can be disconnected:

1. Shut down the OS to avoid corruption. This process shuts down the VM as well.
2. After the guest is down, right-click the temporary VM and click **Edit Settings...**
3. Select the cloned disk, and click **Remove**
4. The Virtual Machine Properties window gives you two options. As the LUN is intended to be removed later, there is no need to destroy the data. So we select **Remove from virtual machine** as in Figure 10-33, then click **OK**.

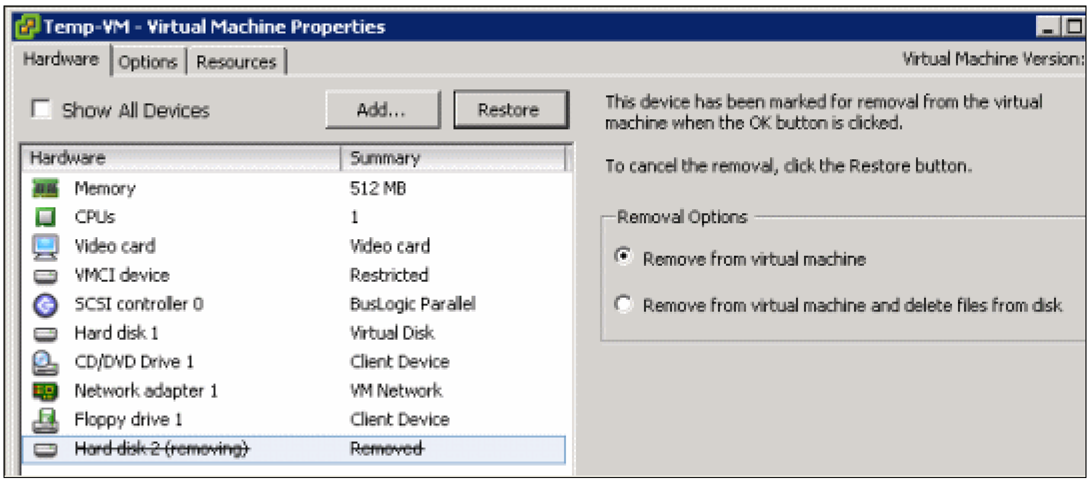



*Figure 10-33 Removing the disk from the VM*

5. Verify that the Recent Tasks list to confirm that the disk was removed, as in Figure 10-34.

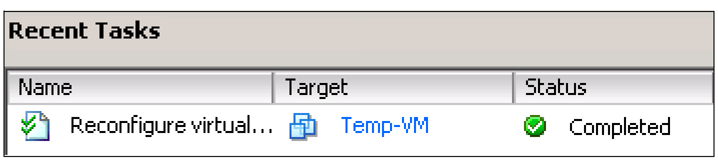



*Figure 10-34 Completion of disk removal*

## 10.4.5 Removing the cloned LUN

After the recovery of the VMware guest or data from the cloned LUN, you must delete the cloned LUN so that N series Snapshot backups can be started again.

**Preparation:** Ensure that any VMware guests that were connected to the cloned LUNs are disconnected before deleting the clone.

To remove the clone, follow these steps:

1. In FilerView, from the left navigation pane (Figure 10-35), select **Volumes** → **Manage**. Select the cloned volume and click **Offline**, as shown in Figure 10-35.

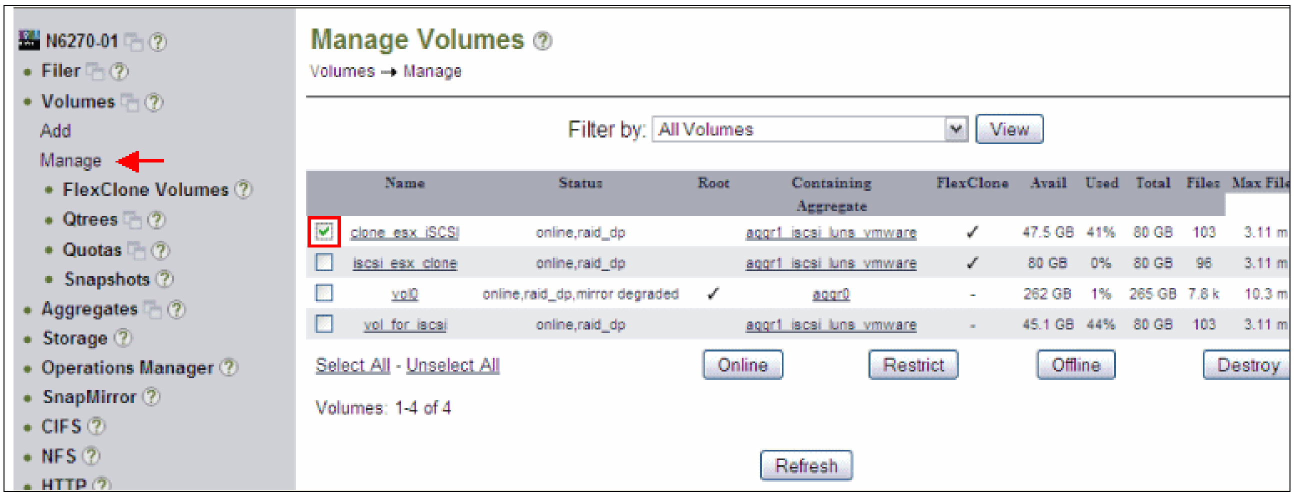



*Figure 10-35 Selecting the volume and taking it offline*

2. Click **OK** to confirm taking the volume offline and then check the success message on Manage Volumes, as in Figure 10-36.

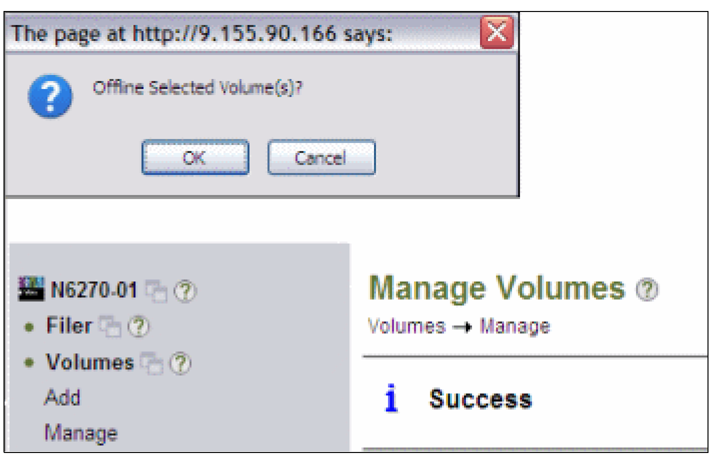



*Figure 10-36 Take volume offline*

3. Select the volume again, but this time, click the **Destroy** button.
4. Click **OK** to confirm that you want to destroy the volume that is shown.

5. Now the Manage Volumes pane (Figure 10-37) indicates that Destroy function was successful, and the volume is not present on the list anymore.

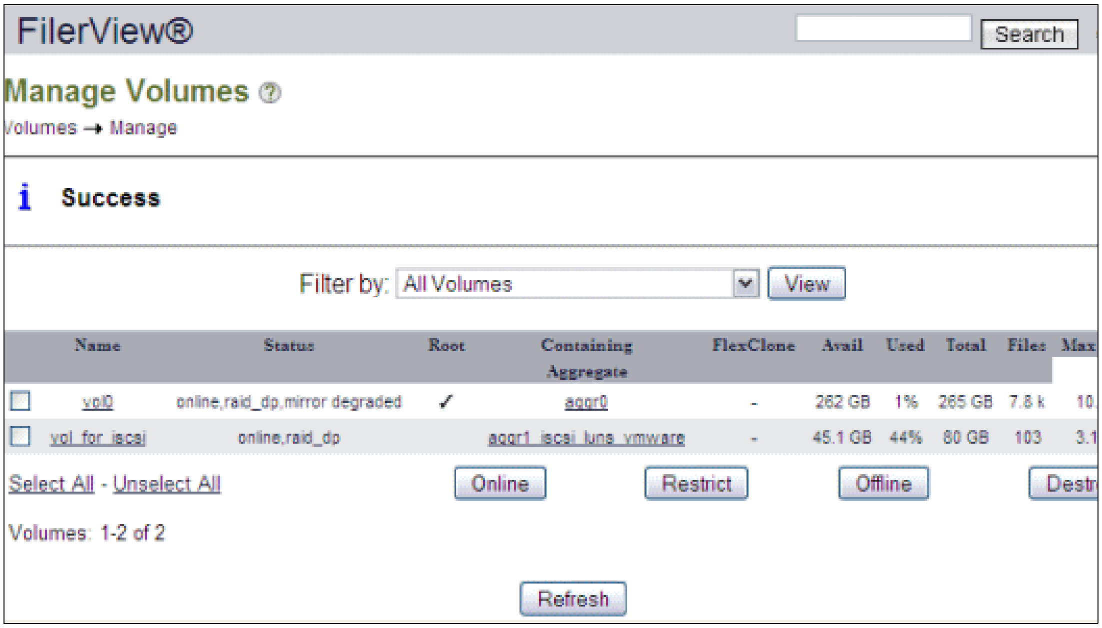



Figure 10-37 The success message after destroying the volume

6. You will see the datastore related to that LUN grayed, as it is unavailable (Figure 10-38).

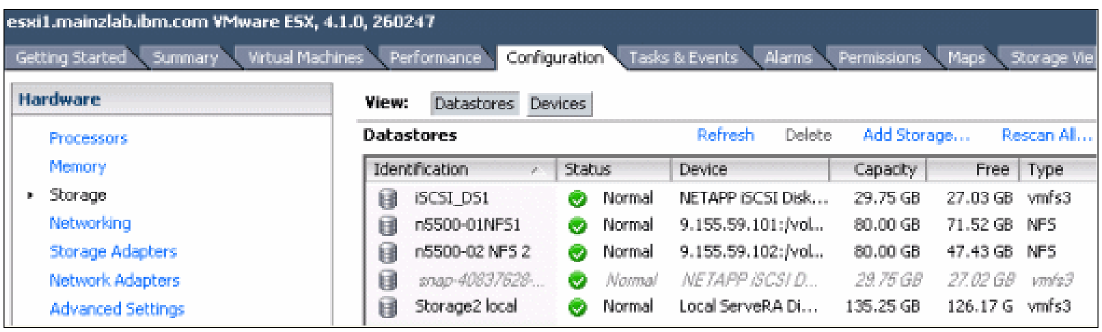



Figure 10-38 Datastore grayed due to LUN unavailability

7. Click **Rescan All...** to remove that datastore from the list, as shown in Figure 10-39.

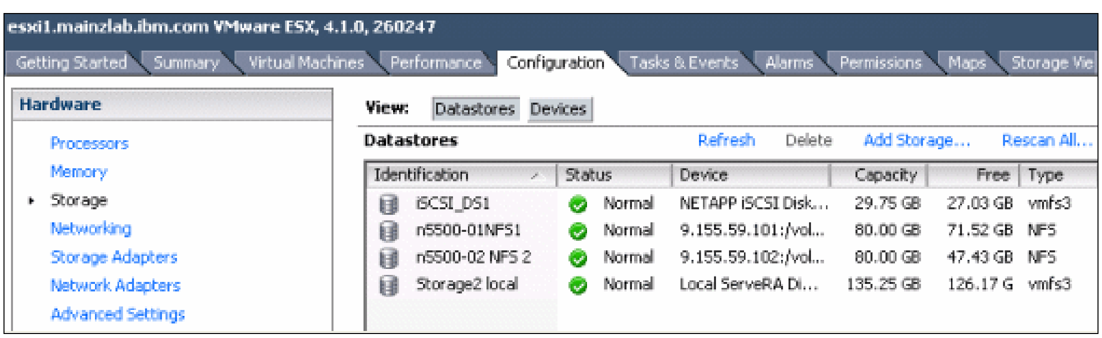



Figure 10-39 Grayed datastore not on the list anymore after a rescan

# 11

# Backup and recovery to a separate system

The N series storage systems provide a facility called *SnapVault*. It uses the Snapshot principles to make copies of the data of the primary storage system and put them onto a secondary system. With this method, the secondary system can replace tape backup for normal backup operations.

However, if tape is required, for example, with long data retention periods, tape backups can be taken off the secondary system. This task does not require a special out-of-hours backup window, because backups do not impact the primary system.

This chapter includes the following topics:

- Licensing the SnapVault locations
- Setting up the primary storage
- Creating a Qtree
- Setting up auxiliary storage
- Configuring SnapVault
- Taping backups from the SnapVault secondary system
- Restoring SnapVault snapshots

## 11.1 Licensing the SnapVault locations

To use SnapVault, you must license the primary and secondary SnapVault locations:

- You enable SnapVault Primary on the N series server that you will back up from (source).
- You also enable SnapVault Secondary on the N series to which you intend to back up.

To license the SnapVault locations, follow these steps:

1. In the left navigation pane of FilerView, select **Filer** → **Manage Licenses**.
2. In the SnapVault ONTAP Primary field (Figure 11-1), enter your primary license.

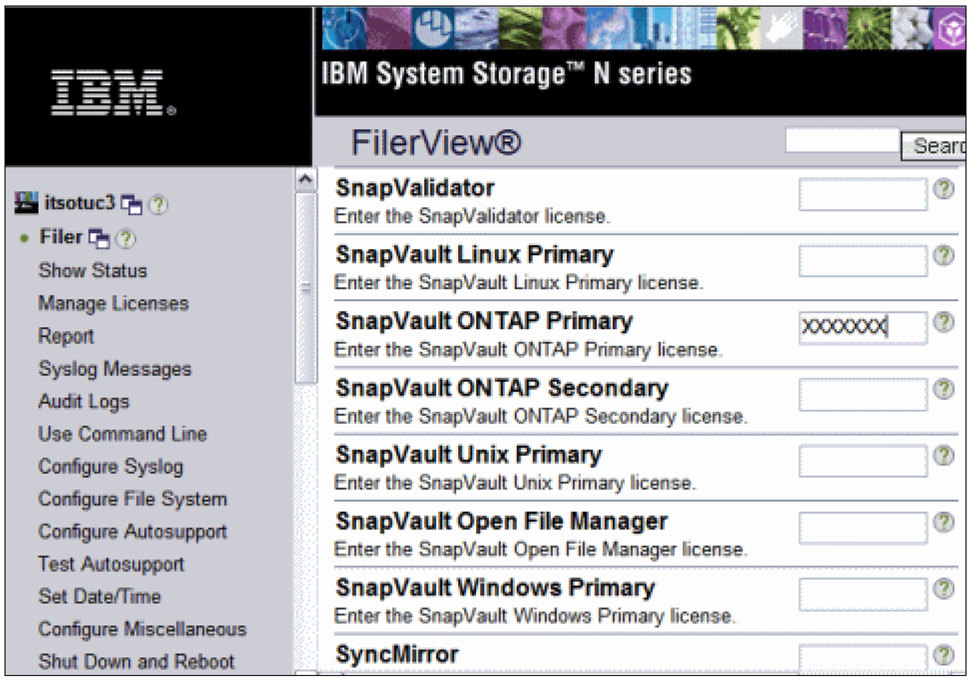



*Figure 11-1 Entering the SnapVault license*

3. Verify that the license was installed successfully (Figure 11-2).

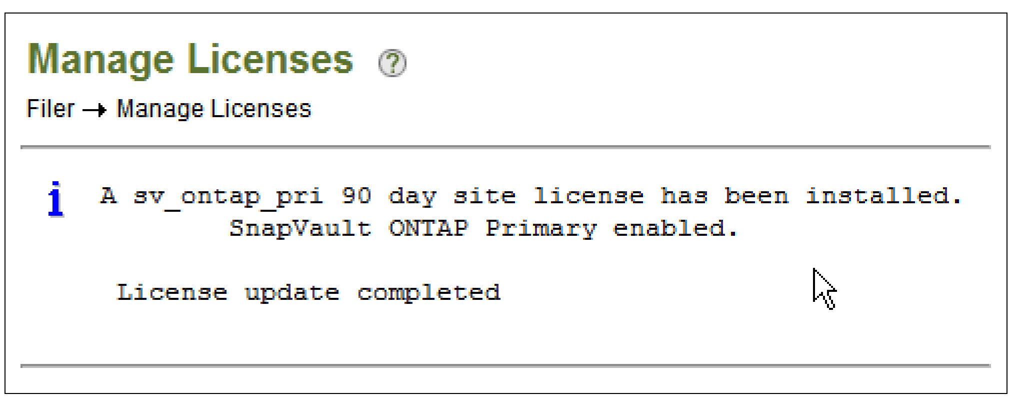



*Figure 11-2 SnapVault license installed*

4. Repeat these steps on the secondary system, entering the license details into the SnapVault ONTAP Secondary field.

## 11.2 Setting up the primary storage

If you are setting up a new environment, you can plan your primary storage based upon the backup schedule that you require. Where possible, co-locate data with similar backup requirements together on the same volumes. Or more importantly, try not to store data with separate requirements on the same volume. For example, make sure that your transient data is stored on separate volumes from your vital data.

The steps for setting up your primary storage are similar to setting up any N series storage for Virtual Infrastructure 4. See Chapter 10, “Recovery options” on page 177. The difference is that storage that is to be replicated by using SnapVault requires an extra level between the volume and the LUN called a *Qtree*. A Qtree provides additional flexibility to assign the specific LUNs to be backed up and restored.

**Volumes without LUNs:** Volumes without LUNs do not require a Qtree on the primary storage. Snapshots are taken at the volume level.

## 11.3 Creating a Qtree

After you create your volumes (or if you have existing volumes), each of them will need at least one Qtree. Do these steps:

1. In FilerView, select **Volumes** → **Qtrees** → **Add** (Figure 11-3).

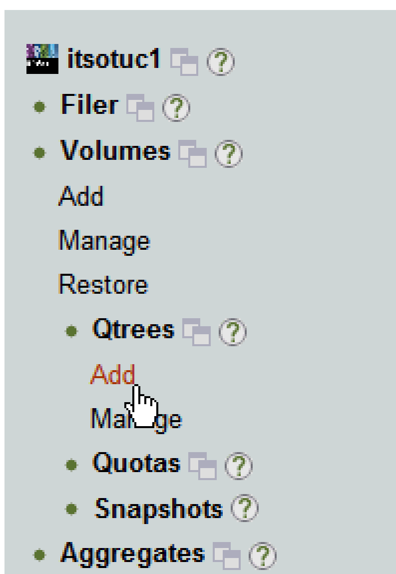



*Figure 11-3 Adding a Qtree*

2. In the Add QTree pane (Figure 11-4), enter the volume in which you want the Qtree to be created, and the Qtree name. Then click **Add**.

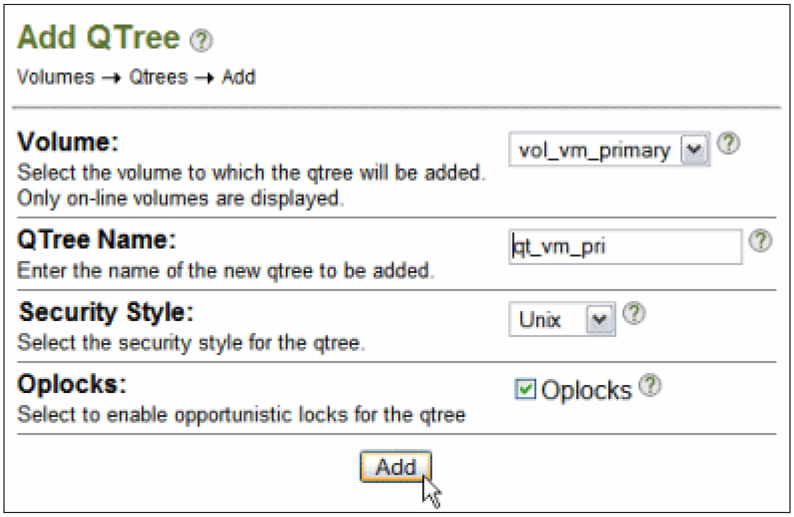



*Figure 11-4 Qtree properties*

3. Verify that the Qtree was created successfully (Figure 11-5).


*Figure 11-5 Qtree created*

4. If you did not yet create LUNs in the volume, create them now. Specify the Qtree in the path by using the following syntax:

```
/vol/<vol_name>/<qtree_name>/<lun_name>
```

For example, the LUN shown in Figure 11-6 is being created in the Qtree created in Figure 11-6.

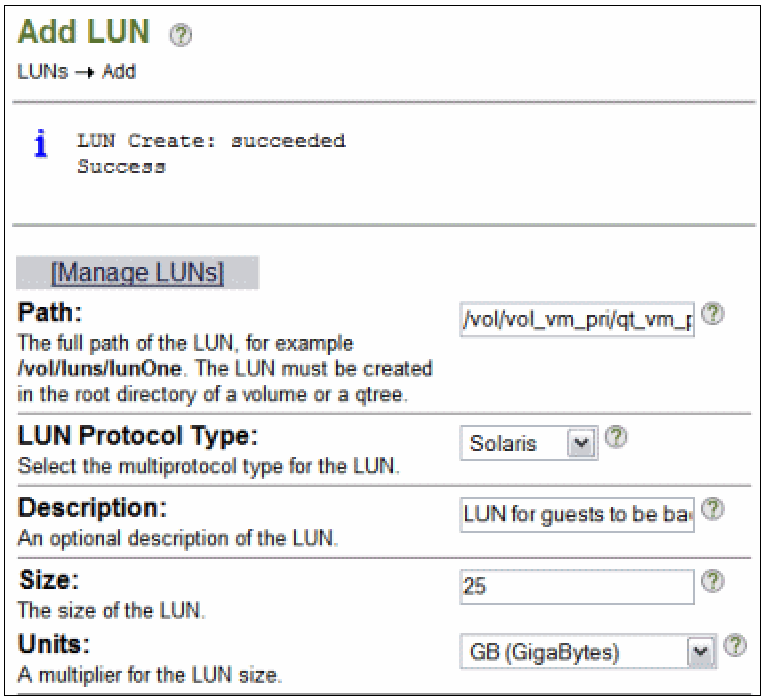



*Figure 11-6 Creating a LUN in the Qtree*

5. If your LUN exists in the volume, change the path. In the left navigation pane of FilerView, select **LUNs** → **Manage**. The LUN shown in Figure 11-7 was moved into a Qtree.

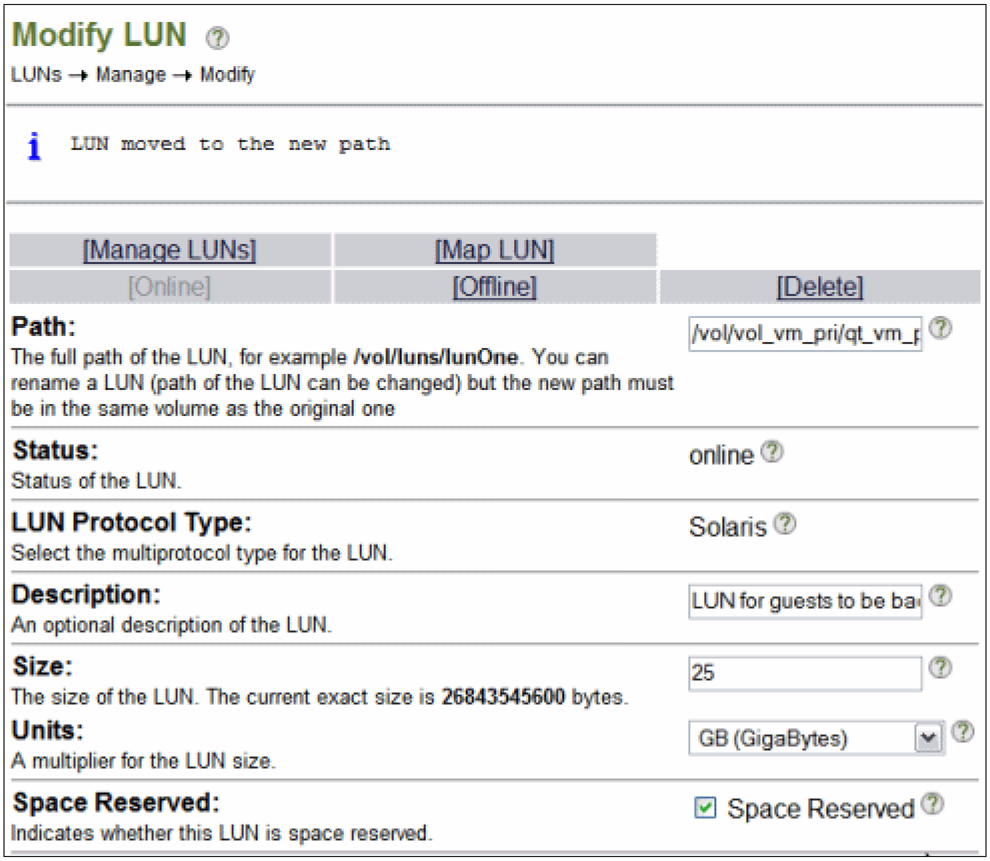



*Figure 11-7 LUN moved to a Qtree*

## 11.4 Setting up auxiliary storage

After your primary storage is configured correctly, set up the auxiliary storage, which is where the backups are to be stored. The auxiliary storage must be configured with a volume at least as large as, or larger than, each primary volume that you intend to back up. You must set the Snapshot reserve to 0.

To set up auxiliary storage, follow these steps:

1. Disable scheduled Snapshots on the volume, because you will use SnapVault for any backups that are required. In FilerView, in the left navigation pane (Figure 11-8), select **Volumes** → **Snapshots** → **Configure**.

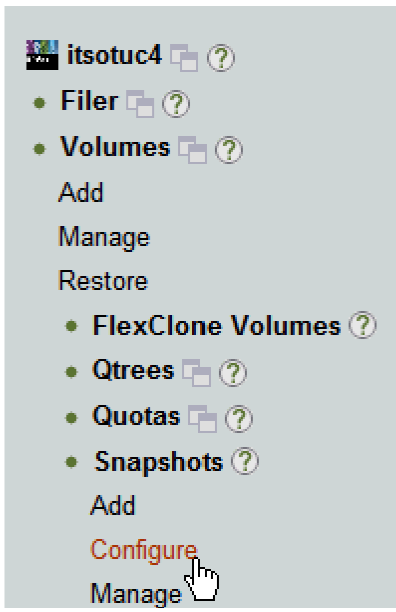



*Figure 11-8 Selecting to configure the Snapshot schedule*

2. In the Configure Snapshots pane (Figure 11-9), select the secondary volume that you just created. For Scheduled Snapshots, clear the **Scheduled** check box.

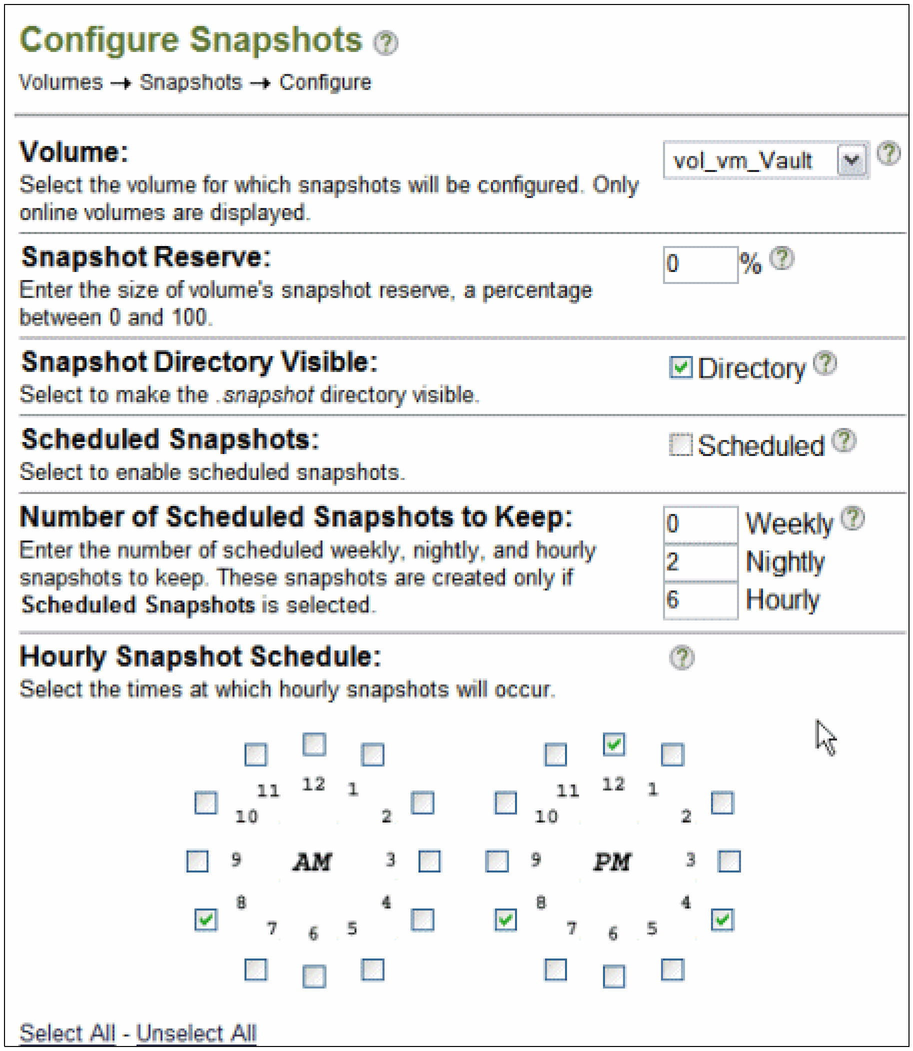



*Figure 11-9 Disabling the schedule*

3. Verify that the Snapshot configuration was successful (Figure 11-10).

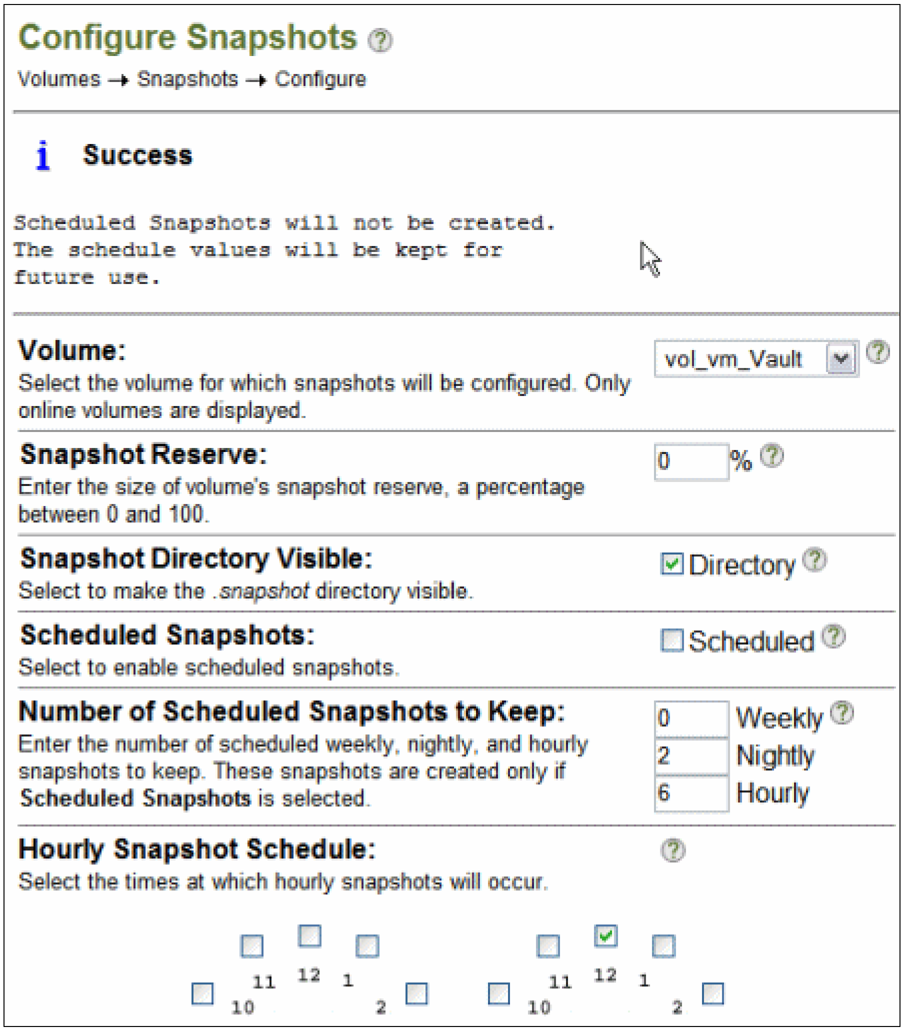



*Figure 11-10 Snapshot schedule not set*

You do not need to set up any Qtrees on the secondary volume. SnapVault creates the Qtrees for you.

## 11.5 Configuring SnapVault

To configure backups using SnapVault, you must perform an initial backup to put the data on the secondary system. Then you must set up a schedule for ongoing SnapVault Snapshots. You can configure this schedule for as often as once each hour, depending on your backup needs.

## 11.5.1 Running the CLI

SnapVault configuration is done by using the N series command line interface (CLI). To run the CLI, use telnet to access the IP address of the N series server. Alternatively, start the command line from FilerView by selecting **Filer** → **Use Command Line** from the navigation pane (Figure 11-11).

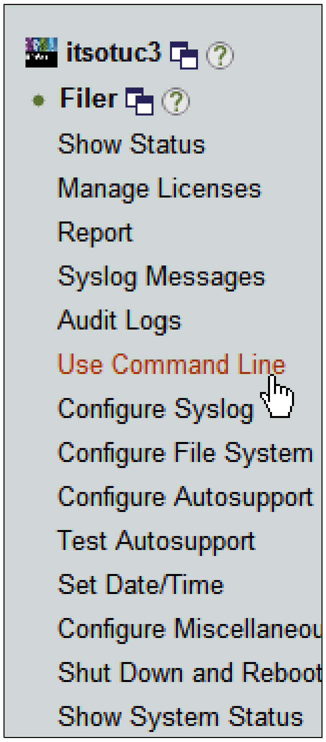



*Figure 11-11 Choosing the CLI option*

The examples in the following sections show commands that you can run on either the primary or secondary system. Therefore, you need to have the CLI open on both systems while doing the configuration.

## 11.5.2 Setting permissions

Set the permissions to allow the secondary system to access SnapVault on the primary system by using the following command on the primary system (Example 11-1):

```
options snapvault.access host=<secondary>
```

*Example 11-1 Setting SnapVault permissions*

```
itsotuc3> options snapvault.access host=9.11.218.238
itsotuc3>
```

Enter the same command on the secondary system, specifying the primary as the host:

```
options snapvault.access host=<primary>
```

By using this command, the primary can perform restore operations from the secondary system later.

### 11.5.3 Performing an initial SnapVault transfer

To perform the initial SnapVault transfer, follow these steps:

1. Set up the initial backup by entering the following command on the secondary system (Example 11-2 on page 207):

   ```
   snapvault start -S <primary>:<primary_qtree> <secondary>:<secondary_qtree>
   ```

   The secondary Qtree does not exist yet. It is created with the name you provide in the command.

   *Example 11-2 Initial SnapVault*

   ```
   itsotuc4*> snapvault start -S 9.11.218.237:/vol/vol_vm_5/qtree_vm1
   itsotuc4:/vol/vol_vm_Vault/qtree_vm_Vault1
   Snapvault configuration for the qtree has been set.
   Transfer started.
   Monitor progress with 'snapvault status' or the snapmirror log.
   ```

   The initial SnapVault might take some time to create, depending on the size of the data on the primary volume and the speed of the connection between the N series systems.

2. Use the **snapvault status** command to check whether the SnapVault is completed (Example 11-3).

   *Example 11-3 Checking the SnapVault Status: Initial SnapVault in progress*

   ```
   itsotuc4*> snapvault status
   Snapvault secondary is ON.
   Source                                  Destination
   State          Lag        Status
   9.11.218.237:/vol/vol_vm_5/qtree_vm1 itsotuc4:/vol/vol_vm_Vault/qtree_vm_Vault1
   Uninitialized  -          Transferring  (4086 MB done)
   itsotuc4>
   ```

   After the initial SnapVault is complete, the **snapvault status** command is displayed as *idle* (Example 11-4).

   *Example 11-4 Check SnapVault Status - Initial SnapVault complete*

   ```
   itsotuc4> snapvault status
   Snapvault secondary is ON.
   Source                                  Destination
     State          Lag        Status
   9.11.218.237:/vol/vol_vm_5/qtree_vm1  itsotuc4:/vol/vol_vm_Vault/qtree_vm_Vault1
   Snapvaulted    00:38:27   Idle
   itsotuc4>
   ```

3. Check the volumes on the secondary system in FilerView to ensure that they are using the expected amount of space. They need about the same amount as on the primary system.
4. Check that the Qtree created by the initial SnapVault is listed in FilerView.

You are now ready to set up the SnapVault schedule for automated Snapshot transfers for the future.

## 11.5.4 Configuring the schedule

Unlike the initial setup of SnapVault, the schedules are configured at the volume level rather than at the Qtree level. The schedule must be configured on both the primary and auxiliary storage systems. This way, the primary system can create a Snapshot locally and then the destination transfers the data across to itself.

### Setting up the primary schedule

Set up the SnapVault schedule on the primary system by entering the following command on the primary system:

```
snapvault snap sched <volume_name> <snap_name> <sched_spec>
where <sched_spec> is <copies>[@<hour_list>][@<day_list>]
```

For example, you might want to schedule snapshots to run three times a day at 8 a.m., 4 p.m., and midnight, retaining two days worth of backups (that is, six copies). Example 11-5 shows the command and resulting output for this configuration.

*Example 11-5 Scheduling SnapVault Snapshots on the primary system*

```
itsotuc1> snapvault snap sched vol_vm_pri 8_hourly 6@0,8,16
itsotuc1> snapvault snap sched
create vol_vm_pri 8_hourly 6@0,8,16
itsotuc1>
```

Use the **`snapvault snap sched`** command to check the newly created schedule.

### Setting up the secondary schedule

You must also configure the schedule for the auxiliary storage system in a similar way. However, the secondary needs to transfer the snapshot from the primary system. Therefore, the command is a little different:

```
snapvault snap sched -x <volume_name> <snap_name> <sched_spec>
where <sched_spec> is <copies>[@<hour_list>][@<day_list>]
```

The **`-x`** option tells the secondary system to transfer the snapshot from the primary system.

In the previous example, where three backups are taken per day, you might want to retain backups on the secondary system for a longer period. For example, you might want to retain backups for a week (that is, 21 backups in total). Example 11-6 shows the command and resulting output in this situation.

*Example 11-6 Scheduling SnapVault Snapshot transfers on the secondary system*

```
itsotuc4> snapvault snap sched -x vol_vm_vault2 8_hourly 21@0,8,16
itsotuc4> snapvault snap sched
xfer   vol_vm_vault2 8_hourly 21@0,8,16
itsotuc4>
```

After the scheduled time passes, look for your Snapshots in FilerView on both the primary and auxiliary storage systems. Their names are based on the snap_name that you set previously. Figure 11-12 shows an example from the secondary system.

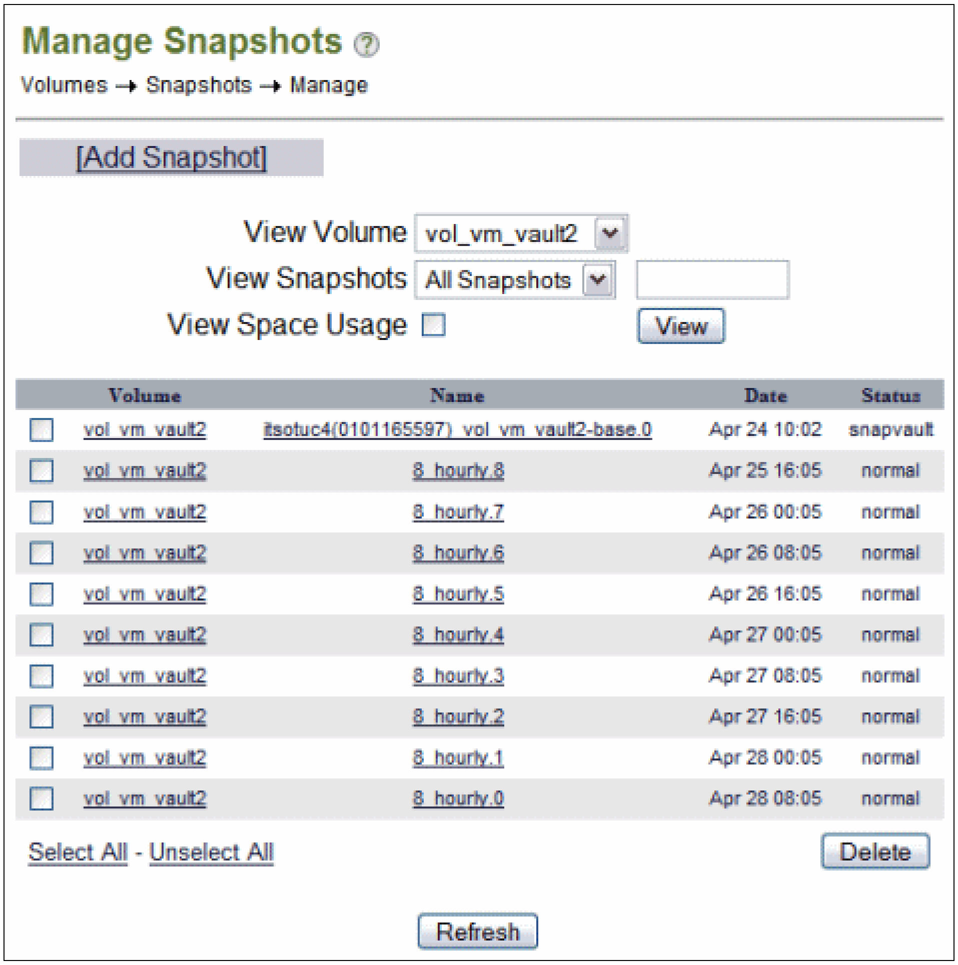



*Figure 11-12 SnapVault Snapshots in FilerView*

## 11.5.5 Scripting a schedule

Similar to regular snapshots, you take VMware guest snapshots before the SnapVault scheduled Snapshot or transfer to provide a consistent, recoverable guest state.

You can script this schedule by using the following Virtual Infrastructure 3 commands:

- The **`snapvault snap sched`** command is used to set the retention.
- The **`snapvault snap create`** command is used to create the snapshots.

You still perform the initial snapshot from the secondary system as described previously. Then you run the **`snapvault snap sched`** command once on the primary system to set the retention of the snapshots to be scripted. Do not specify the times to run (Example 11-7).

*Example 11-7 SnapVault Snapshot retention on the primary system*

```
itsotuc1> snapvault snap sched vol_vm_pri 8_hourly 6@-
itsotuc1> snapvault snap sched
create vol_vm_pri 8_hourly 6@-
itsotuc1>
```

The VMware and SnapVault script can now be run on the primary system by using the same **snapname** specified in the schedule. Example 11-8 shows the **snapvault** command included in the script.

*Example 11-8 SnapVault command in the VMware Snapshot script*

```
itsotuc1> snapvault snap create vol_vm_pri 8_hourly
itsotuc1>
```

The secondary system can have a normal SnapVault schedule configured that is timed to start a little after the script is run on the primary systems, as shown in Example 11-9.

*Example 11-9 Schedule for SnapVault Snapshot transfers on the secondary system*

```
itsotuc4*> snapvault snap sched -x vol_vm_vault2 8_hourly 21@0,8,16
itsotuc4*> snapvault snap sched
xfer   vol_vm_vault2 8_hourly 21@0,8,16
itsotuc4*>
```

# 11.6 Taping backups from the SnapVault secondary system

Where off-site backup is required, or if longer retention periods exist than are economical to store on disk, snapshots from the auxiliary storage system can be written to tape. You can perform this task by using the N series **dump** command with a local tape system. Alternatively, you can use an NDMP-enabled backup application, such as IBM Tivoli Storage Manager.

The volumes of the auxiliary storage system can be mapped directly by the backup server, and the Snapshots are stored as subdirectories. Therefore, you can perform backup to tape of the required snapshots at any convenient time before the snapshot retention period expires.

For details about using Tivoli Storage Manager to back up an N series storage system, see *Using the IBM System Storage N series with IBM Tivoli Storage Manager*, SG24-7243.

# 11.7 Restoring SnapVault snapshots

Similar to regular snapshots, the type of recovery is determined by the level of restoration that is required. This section explains how to recover a Qtree from a SnapVault Snapshot. The concepts for recovering a virtual machine or file within a virtual machine are the same as for regular snapshots. For additional information about some of these procedures, see Chapter 10, “Recovery options” on page 177.

## 11.7.1 Preparation

If you did not do so already, set the permissions on the secondary to allow the primary to perform the restore by entering the following command on the secondary system (Example 11-1 on page 206):

```
options snapvault.access host=<primary>
```

Before recovering SnapVault Snapshots to Virtual Infrastructure 4.x, the ESX host must be configured to allow Volume Resignaturing.

## 11.7.2 Restoring the Qtree

Performing a LUN restore from SnapVault places the restored LUN on a volume on the primary storage system. You enter the following command (Example 11-10) from the primary system:

```
snapvault restore -S <secondary>:<secondary_qtree> <destination_qtree>
```

The destination Qtree does not yet exist. It is created with the name you provide in the command. This command restores all LUNS from the secondary Qtree to the new Qtree. The new Qtree can be in the same volume or in a different volume from the original source data.

*Example 11-10 SnapVault restore command*

```
itsotuc1> snapvault restore -S 9.11.218.238:/vol/vol_vm_vault2/qt_vm_vault2
/vol/vol_vm_pri/qt_rest1
Restore from 9.11.218.238:/vol/vol_vm_vault2/qt_vm_vault2 to
/vol/vol_vm_pri/qt_rest1 started.
Monitor progress with the 'snapvault status' command.
Abort the restore with ^C.
```

The CLI for the primary system is unavailable for commands until the restore is complete. Alternatively, you can press Ctrl+C to end the restore. To view the status, use the **snapvault status** command on the secondary system as shown in Example 11-11.

*Example 11-11 SnapVault status: Restore underway*

```
itsotuc4> snapvault status
Snapvault secondary is ON.
Source                                  Destination
      State          Lag        Status
9.11.218.114:/vol/vol_vm_pri/qt_vm_pri  itsotuc4:/vol/vol_vm_vault2/qt_vm_vault2
    Snapvaulted    04:13:04   Idle
itsotuc4:/vol/vol_vm_vault2/qt_vm_vault2  itsotuc1:/vol/vol_vm_pri/qt_rest1
      Source         -          Transferring  (3991 MB done)
itsotuc4>
```

As with the initial Snapshot, the restore might take some time, depending on how much data in the Qtree is restored. When it is completed, the primary CLI shows a success message and becomes available again (Example 11-12).

*Example 11-12 Successful restore*

```
Made qtree /vol/vol_vm_pri/qt_rest1 writable.
Restore to /vol/vol_vm_pri/qt_rest1 completed successfully.
itsotuc1>
```

The secondary system also shows that the restore is complete, when using the **snapvault status** command (Example 11-13).

*Example 11-13 SnapVault Status: Restore completed*

```
itsotuc4> snapvault status
Snapvault secondary is ON.
Source                                  Destination
    State          Lag        Status
9.11.218.114:/vol/vol_vm_pri/qt_vm_pri  itsotuc4:/vol/vol_vm_vault2/qt_vm_vault2
  Snapvaulted    04:27:37   Idle
itsotuc4:/vol/vol_vm_vault2/qt_vm_vault2  itsotuc1:/vol/vol_vm_pri/qt_rest1
    Source         04:13:36   Idle
itsotuc4>
```

## 11.7.3 Restoring a previous backup

You saw how to restore from the most recent SnapVault backup that exists on the secondary system in 11.7, “Restoring SnapVault snapshots” on page 210. To restore from a previous backup version, enter the following command:

```
snapvault restore -s <secondary_snapname> -S <secondary>:<secondary_qtree>
<destination_qtree>
```

Here is how to find the secondary snapshot name for the volume where the required Qtree is on the secondary system. In FilerView on the secondary system, select **Volumes** → **Snapshots** → **Manage**. The name must be the name that you gave the snapshot on the secondary SnapVault schedule. It must be appended with a number to show which retained version it is, where the numbers start from zero. For example, the most recent version is 0, the previous backup was 1. The command shown in Example 11-14 restores the third most recent backup from the secondary system to a different volume from the original.

*Example 11-14 Restoring a previous SnapVault backup*

```
itsotuc1> snapvault restore -s 8_hourly.2 -S
9.11.218.238:/vol/vol_vm_vault2/qt_vm_vault2 /vol/vol_vm_rest/qt_rest1
Restore from 9.11.218.238:/vol/vol_vm_vault2/qt_vm_vault2 to
/vol/vol_vm_rest/qt_rest1 started.
Monitor progress with the 'snapvault status' command.
Abort the restore with ^C.
Made qtree /vol/vol_vm_rest/qt_rest1 writable.
Restore to /vol/vol_vm_rest/qt_rest1 completed successfully.
itsotuc1>
```

## 11.7.4 Mapping the LUN

After the restore is completed, the restored LUNs are displayed in the new Qtree on the primary system. You must map the required LUNs to allow them to be accessed by the VMware host.

Follow the instructions provided in 10.2.2, “Configuring the cloned LUN to be accessed” on page 183to map the LUNs.

### 11.7.5 Mounting a restored image in the VMware host

After the LUN is mapped, rescan the adapters on the VMware hosts, as explained in 10.2.2, "Configuring the cloned LUN to be accessed" on page 183. The data is now accessible. Depending on the restoration you require, perform one of the following actions:

- Start the restored guests from the restored location:

  a. Check that the original guests are no longer running, or stop them.
  a. Open the recovered datastore on an ESXi host.
  b. Add each guest to the inventory.
  c. Start the recovered guests.

- Copy the required guests across to an existing datastore:

  a. Open the original and restored datastores in vCenter.
  b. Copy the required guest folders from the restored datastore to the original datastore.
  c. Start the guests in the original datastore.
  d. Delete the restored Qtree with data.

- Temporarily mount a guest to recover individual guest files:

  a. Connect the .vmdk file of the restored datastore to a temporary guest.
  b. Copy the required files from the restored .vmdk to the original guest.
  c. Disconnect and remove the restored Qtree with data.

12

# High availability and disaster recovery

This chapter provides information about the opportunities for high availability (HA) when using VMware vSphere 4.1 and N series storage in the same environment. It then explains the implementation of disaster recovery using the functions of these technologies.

This chapter includes the following topics:

- High availability
- Disaster recovery options
- Setting up disaster recovery
- Recovering from a disaster
- Returning to production
- Disaster recovery testing

## 12.1 High availability

This section provides details about some of the high availability features of the N series and Virtual Infrastructure 3 solution.

### 12.1.1 N series node failures

In a normal configuration, two N series servers are clustered. If a failure occurs in one of the nodes, the second system automatically takes on the load of both servers without any manual intervention required.

However, if a failure affects both nodes, such as a power failure for the whole server environment, a disaster recovery implementation is required. This implementation can be in the form of a second pair of N series servers in a location nearby, using MetroCluster. Or it can be done with a pair of N series servers in a more remote location, using SnapMirror.

An N series cluster (standard N series configuration) offers the following high availability features:

- Built-in redundancy for a failure of a power supply, fan, or disk controller
- RAID-DP for a single or dual disk failure
- Multipath for a single disk path or port failure
- Snapshot copies for accidental erasure or destruction of data

MetroCluster is an extended N series cluster for distances of up to 100 km with fiber connectivity between sites. It provides the following additional HA features:

- SyncMirror for a triple disk failure or complete disk shelf failure
- Redundancy for a host bus adapter (HBA) or port failure
- Active-active controller configuration for a storage controller failure
- MetroCluster for a data center power or environmental outage
- The ability of VMware HA cluster to be split across the MetroCluster

Figure 12-1 shows a fabric attached MetroCluster configuration.

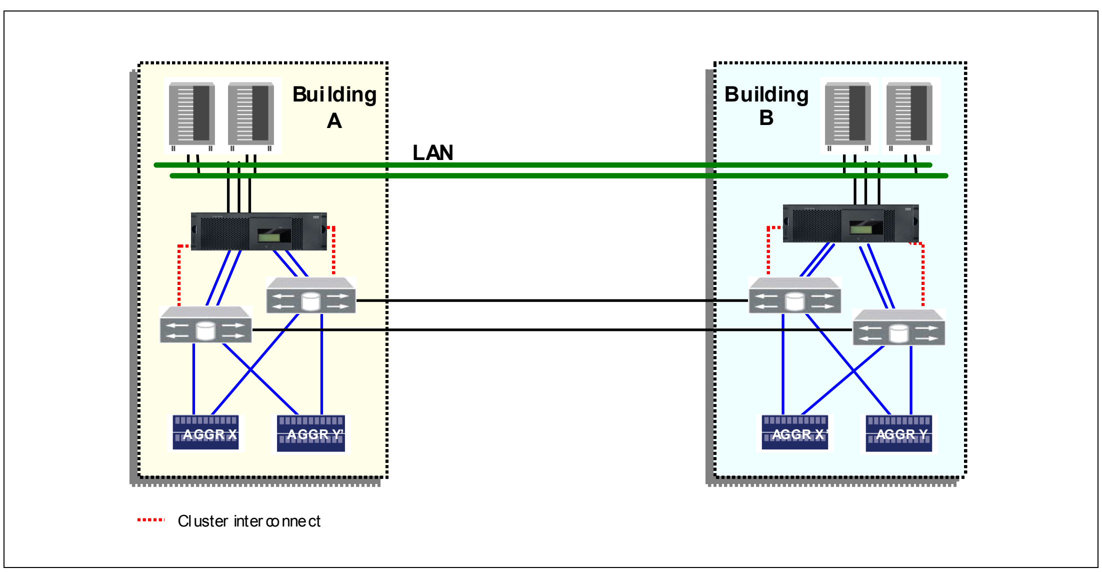



*Figure 12-1 MetroCluster configurations*

### 12.1.2 VMware host failures

With two or more VMware hosts configured in a cluster with a shared storage, you can have high availability features. Virtual machines on a failed host can be quickly restarted on another host, as long as there is capacity available on the remaining hosts. This feature is enabled by VMware High Availability (HA). As a preferred practice, provide enough capacity on your environment for the failure of at least one host, also known as N+1. Depending on your availability requirements and the speed of growth of your environment, you might even want to size it N+2.

Another feature available is Dynamic Resource Scheduler (DRS), which manages the load of the guests across the servers in the cluster. If one of the hosts becomes overloaded, guests can be automatically moved to a server with a less load without any downtime. If you plan to use the VMware HA feature, you can also use the DRS feature. This feature allows virtual machines to be evenly balanced across the cluster in the event of a host failure.

If you do not have high availability on your environment, use operating system or application-level clustering. If your application is not state-aware, use load balancers, as for web servers.

## 12.2 Disaster recovery options

You can mirror an N series node (cluster) at the primary site to an N series node at a secondary site (Figure 12-2). It can be used in a development or test capacity during normal operation if the loss of it in a disaster is acceptable. Otherwise, it can be used for on demand or out-of-band additional capacity.

Disaster recovery can also be done using a FlexClone of the SnapMirror. You can even start the virtual machines in the DR site while the run on the primary site if their network is isolated. This method uses a lot less disk than traditional methods, because cloning does not require a full copy of the source, but rather only as changes occur on either copy.

A VMware host or cluster must be in the disaster recover site also to run the VMs present on the cloned storage at DR site. However, it does not have to be the same hardware, thus providing more flexibility to your planning.

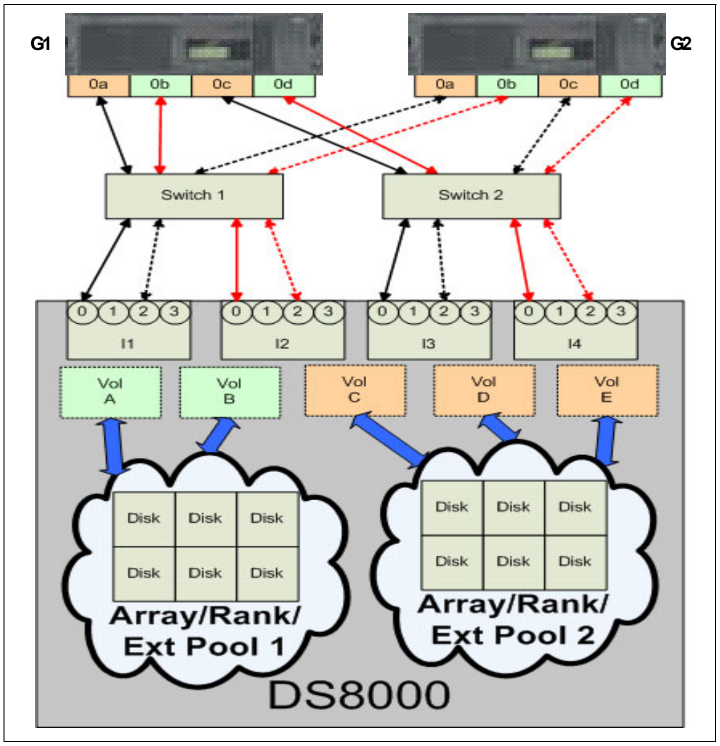



*Figure 12-2 N series Gateway cluster configuration*

# 12.3 Setting up disaster recovery

In this section, you configure a Virtual Infrastructure 3 and N series environment to use the N series SnapMirror feature. This feature provides replication of the datastores to a second location that is ready for use in the event of a disaster.

The following tasks are involved:

1. Configuring the source location storage
2. Enabling SnapMirror on the N series storage systems
3. Configuring the mirror
4. Starting the mirror

The SnapMirror configuration is similar in many ways to SnapVault configuration. Therefore, if you already reviewed Chapter 11, “Backup and recovery to a separate system” on page 197, you can see that the setup is familiar.

## 12.3.1 Setting up the primary storage

If you are setting up a new environment, you can plan your storage based on your disaster recovery requirements. Where possible, co-locate data with similar disaster recovery requirements on the same volumes. More importantly, try not to store data with separate requirements on the same volume. For example, make sure that your transient data is stored on separate volumes from your vital data.

To set up the primary storage, follow these steps:

1. Set up your primary storage as for any N series storage for VMware.
2. On the destination storage system, create a volume for each volume you intend to replicate that is at least as large as the source volume. However, do not create LUNs, because they are replicated from the source.
3. Restrict access to the destination volumes by entering the **vol restrict <vol_name>** command (Example 12-1). This command prevents the volume from being accessed by the virtual machines outside of a disaster situation.

*Example 12-1 Restricting a destination volume*

```
itsotuc1> vol restrict vol_vm_dr
Volume 'vol_vm_dr' is now restricted.
itsotuc1>
```

4. On the destination storage system, create a volume with the appropriate LUNs that are the same as each of the volumes on the source that contains the transient data.
5. Disable the automatic snapshots of both the source and destination volumes unless you have a separate need for them.

**SnapMirror:** Unlike SnapVault, which requires Qtrees, SnapMirror works at either the Qtree level or volume level. The examples in this section use volumes, but you can use Qtrees instead if you prefer.

## 12.3.2 Licensing SnapMirror

To use SnapMirror, you must apply your site license to the source and destination N series storage systems and to the clustered nodes for each system, if applicable:

1. In FilerView, in the left navigation pane, select **Filer** → **Manage Licenses**.
2. In the Manage Licenses pane (Figure 12-3), enter your license code and select **Apply**.

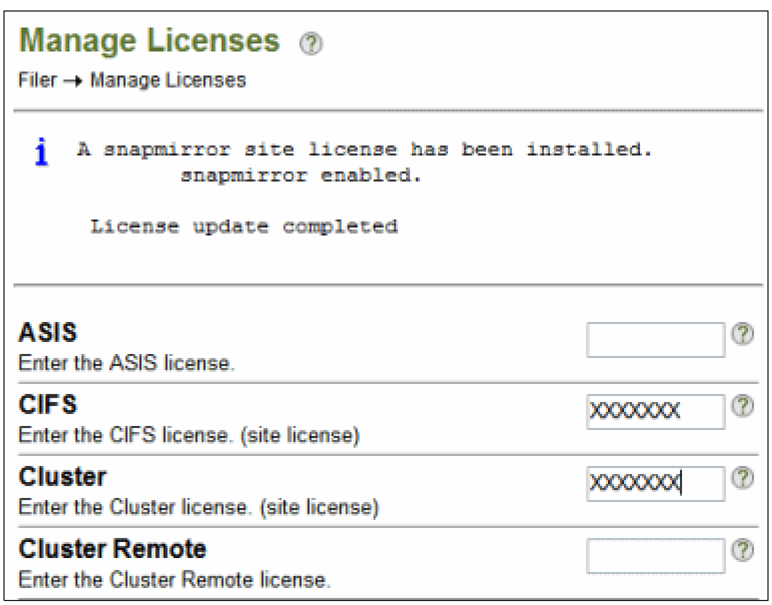



*Figure 12-3 SnapMirror License installed*

When installed, the SnapMirror options become available in the left navigation pane (Figure 12-4) of FilerView.

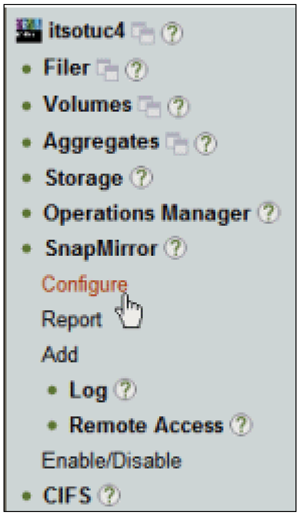



*Figure 12-4 SnapMirror menu options*

## 12.3.3 Setting permissions

Set the permissions to allow the destination system to access SnapMirror on the source by entering the following command on the source system (Example 12-2):

```
options snapmirror.access host=<secondary>
```

*Example 12-2 Setting the SnapVault permissions*

```
itsotuc4*> options snapmirror.access host=9.11.218.114
itsotuc4*> options snapmirror.access
snapmirror.access            host=9.11.218.114
itsotuc4*>
```

The **`options snapmirror.access`** command verifies that the permission was assigned correctly.

You can also use this function in FilerView. In the left navigation pane, select **SnapMirror** → **Remote Access** → **Add**. However, use the CLI command shown in Example 12-2 to confirm that the access was assigned correctly.

## 12.3.4 Configuring the volume mirror

To configure the volume mirror, follow these steps:

1. Set up the mirror transfer from the secondary system. In FilerView, in the left navigation pane (Figure 12-5), select **SnapMirror** → **Add**.

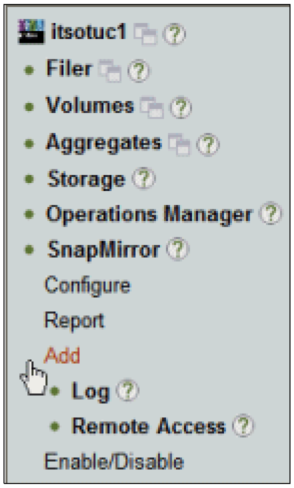



*Figure 12-5 Selecting the option to add SnapMirror*

2. In the Destination Location panel of the SnapMirror Wizard (Figure 12-6), select the destination volume you created for this volume mirror. Then click **Next**.

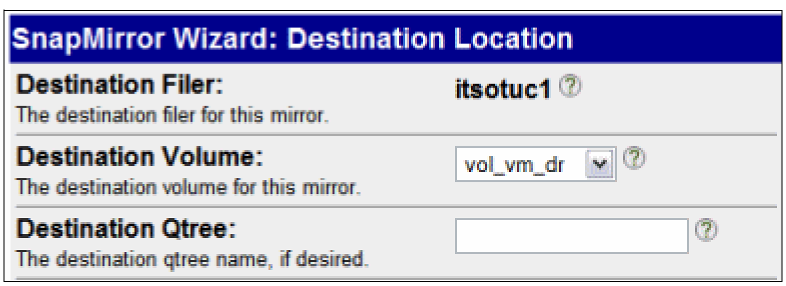



*Figure 12-6 SnapMirror destination*

3. In the Source Location panel shown in Figure 12-7, enter the IP address (or DNS name if you prefer) of the source N series system, and the volume you want to mirror. Then click **Next**.

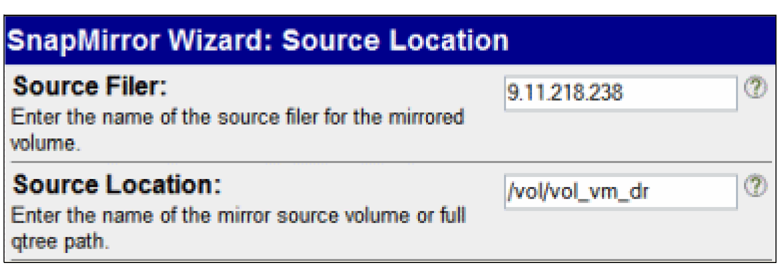



*Figure 12-7 IP address of the remote storage*

4. In the Set Schedule panel (Figure 12-8), limit the transfer rate by selecting how often you want transfer updates to occur, based on your disaster recovery requirements. If you do not want to set any limits, select **Never**. Then click **Next**.

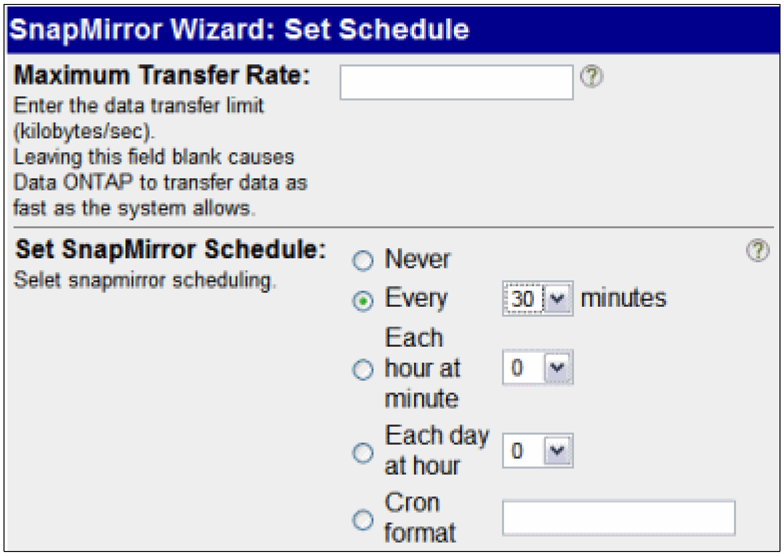



*Figure 12-8 SnapMirror schedule*

5. In the Commit panel (Figure 12-9), verify that the settings you entered are correct. Then click **Commit**.

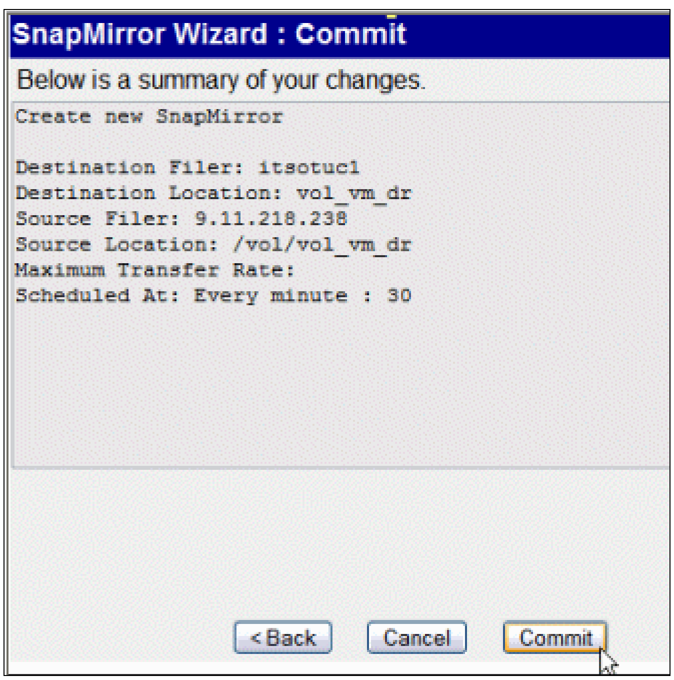



*Figure 12-9 SnapMirror implementation summary*

6. Verify that the SnapMirror was added successfully (Figure 12-10).

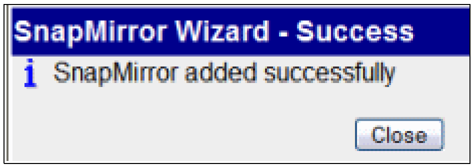



*Figure 12-10 SnapMirror added successfully*

## 12.3.5 Starting a mirror

After you configure the mirror, you must initialize it to start the initial mirror copy to the destination storage system:

1. In FilerView on the destination system, in the left navigation pane (Figure 12-11), select **SnapMirror** → **Report**.
2. In the SnapMirror Report pane (Figure 12-11), select the SnapMirror that you configured. Notice that it is currently not initialized.

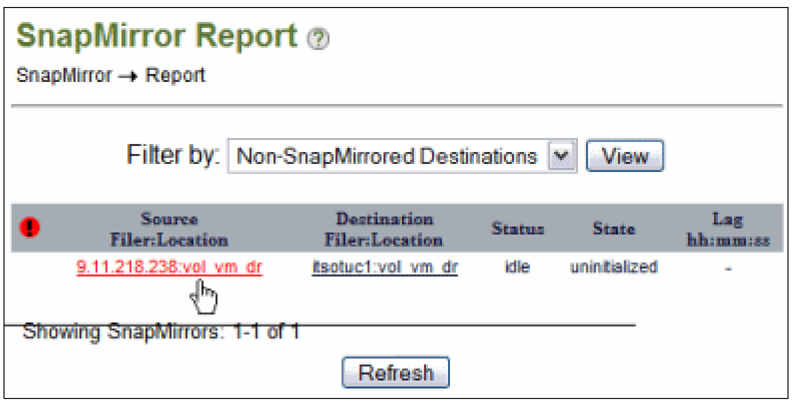



*Figure 12-11 SnapMirror not initialized*

3. In the SnapMirror Properties panel (Figure 12-12), click **Initialize** to start the initial SnapMirror between the two storage systems.

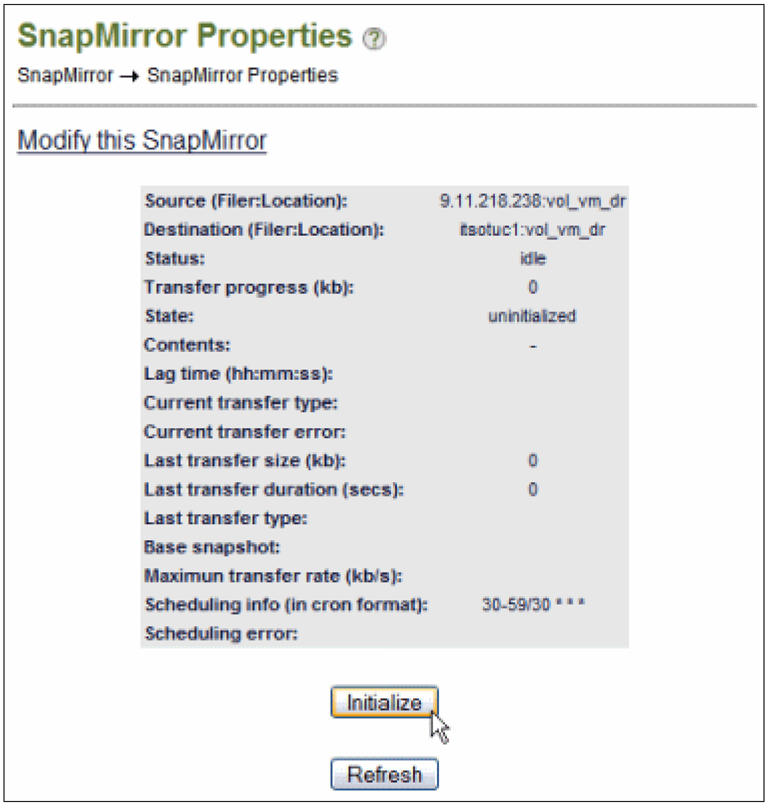



*Figure 12-12 Initializing SnapMirror*

4. In the SnapMirror Properties pane, verify that the initialization process started successfully.
5. Check the SnapMirror Report (Figure 12-13) again for the status. The SnapMirror is idle, because the mirror has been created. Also no scheduled processes are running. You see a similar report on the source server.

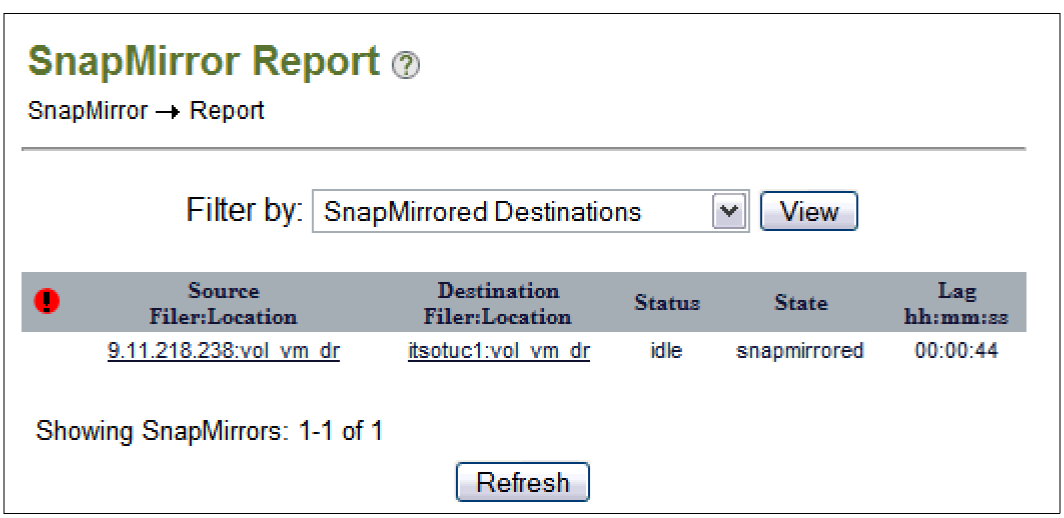



*Figure 12-13 Checking the SnapMirror Report*

You can also check the SnapMirror status in the Manage Snapshots menu:

a. In the left navigation pane of FilerView (Figure 12-14), select **Volumes** → **SnapShots** → **Manage**.


*Figure 12-14 Selecting to manage snapshots*

b. In the Manage Snapshots pane (Figure 12-15), select the SnapMirror volume, and click **View** to see the snapshots for that volume.

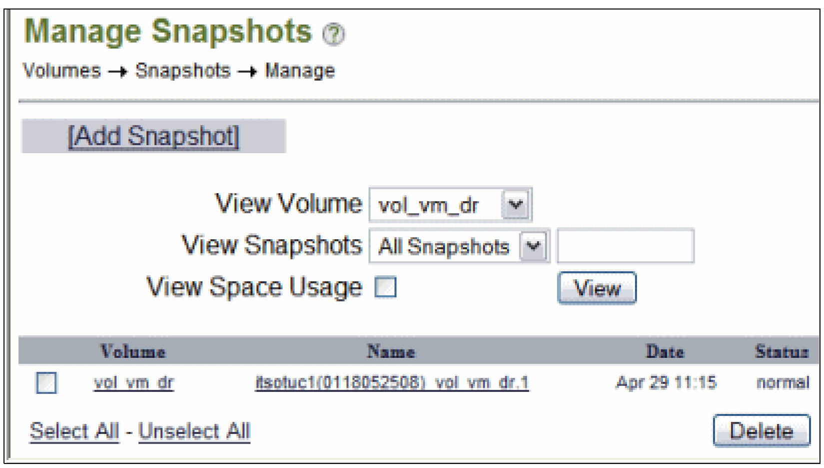



*Figure 12-15 SnapMirror in FilerView*

## 12.4 Recovering from a disaster

If a disaster (or possibly a full test of the disaster recovery capability) occurs, perform the following tasks:

1. Break the mirror to make the mirrored data writable.
2. Map the LUNs.
3. Rescan the VMware hosts to see the LUNs.
4. Reinventory the virtual machines.
5. Start the virtual machines.

## 12.4.1 Breaking the mirror

During the setup procedure, the mirror volumes in the destination location were restricted to prevent writes. To remove this restriction and allow the data to be mounted and accessed, break the mirror:

1. Run FilerView on the destination N series system.
2. In the left navigation pane of FilerView (Figure 12-16), select **SnapMirror** → **Report**.

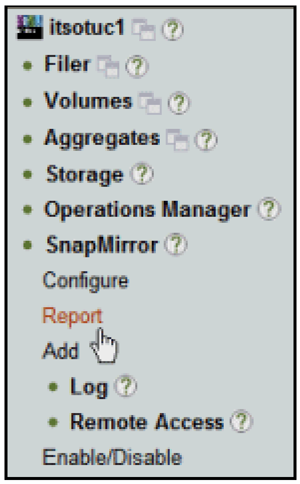



*Figure 12-16 SnapMirror Report*

3. In the SnapMirror Report pane (Figure 12-17), select the volume you want to use.

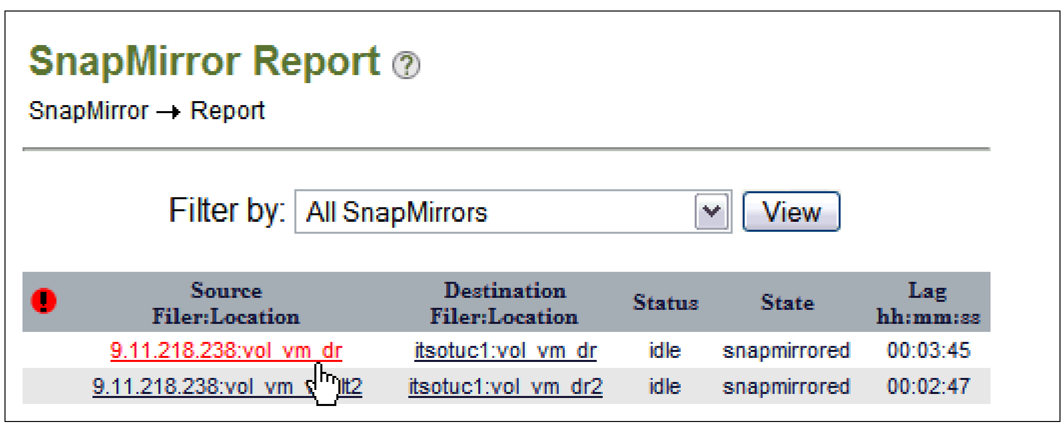



*Figure 12-17 Selecting the volume*

4. In the SnapMirror Properties pane (Figure 12-18), where you see the properties of this volume replica, click **Quiesce** to ensure that no data is unwritten.

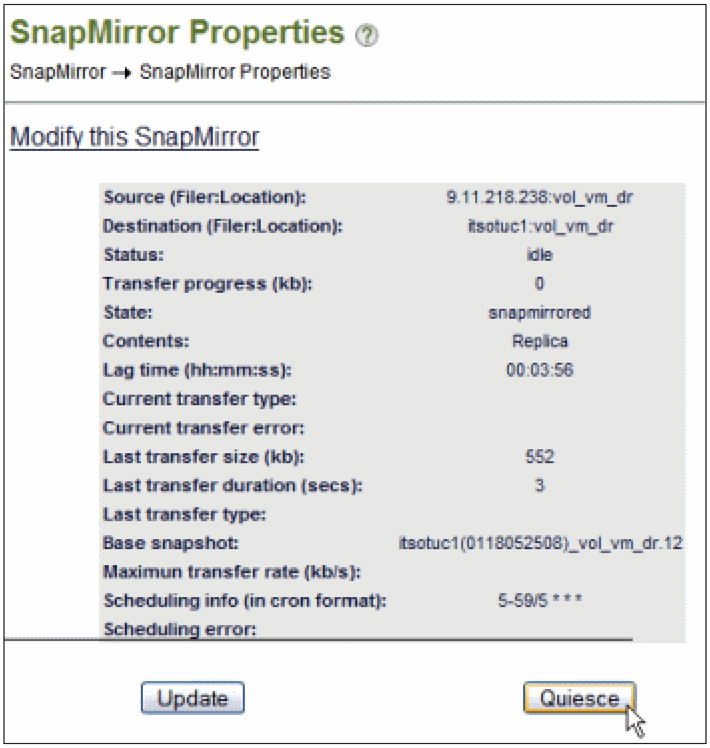



*Figure 12-18 Quiescing the volume*

5. When the quiesce is successful, click **Break** (Figure 12-19).

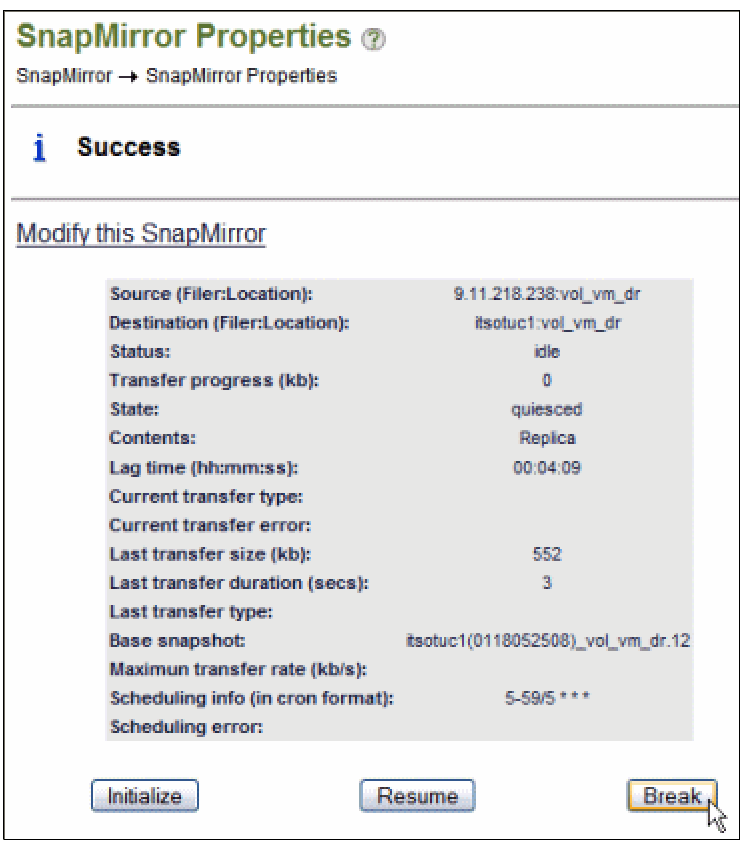



*Figure 12-19 Breaking the mirror*

6. Verify that the break operation completed successfully.
7. Repeat these steps for each mirrored volume that you require access to on the destination system.

### 12.4.2 Mapping the LUNs and rescanning VMware hosts

Now that the mirror is broken and the data is available, any LUNs on the volume must be mapped so that the VMware host can use them.

1. Map the LUN as already previously explained.
2. Create a datastore using the LUN you just mapped.
3. Then reinventory the virtual machines.

Also see the script provided in Appendix A, “Hot backup Snapshot script” on page 279 to help you to perform the tasks.

### 12.4.3 Starting virtual machines

Now that the virtual machines are configured correctly, start them:

1. Right-click a virtual machine and select **Power**, then **Power On**
2. On the right side of the window, when prompted for the Unique Identifier (UUID) settings, select **Create** (Figure 12-20), and click **OK**.

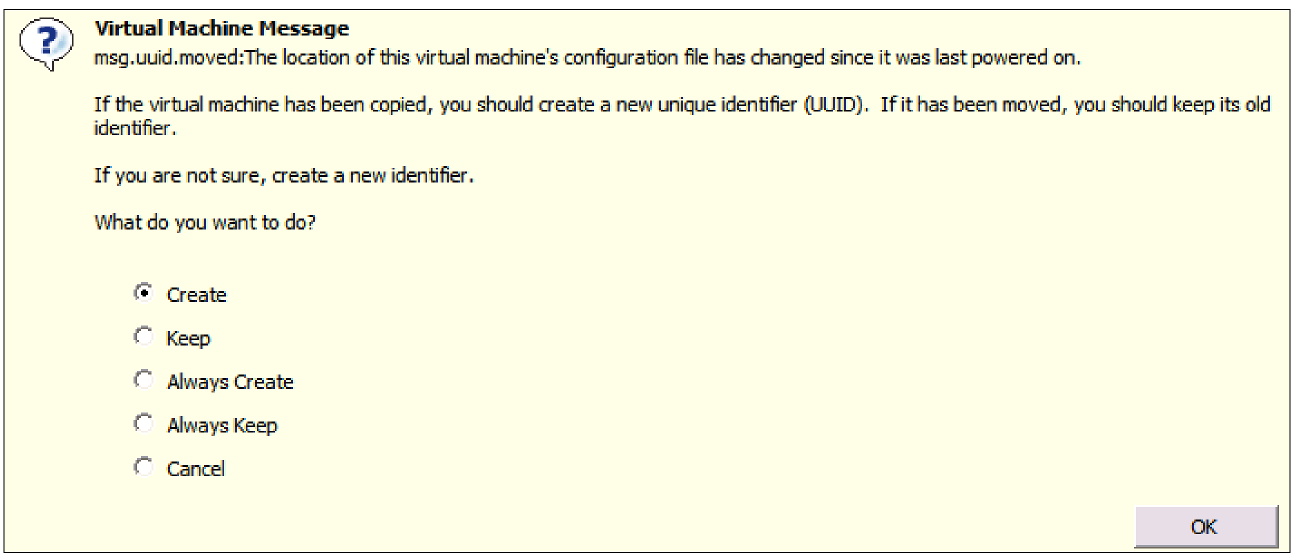



*Figure 12-20 Creating a UUID*

3. Verify the task list to confirm that the guest started correctly (Figure 12-21).

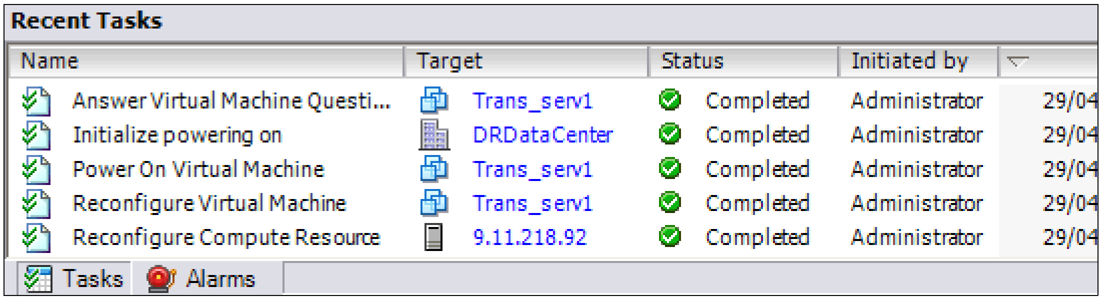


*Figure 12-21 Guest started successfully*

4. Repeat these steps for each guest you want to start in the DR environment. You might also want to start the remote console for the guests, or run application diagnostic tests for each application, to confirm that everything is working as expected.

## 12.5 Returning to production

In a case where a disaster occurred and the environment is failed over to the disaster recovery site, the data stored in there is the most current. If the production environment comes back online later, the data and server load might need to be transferred back. Similar to regular SnapMirror transfers, the production site can be updated from the disaster recovery data while the disaster recovery site is operational. This update might be large if the production data was lost or corrupted, or it might be small if the production data was unaffected by the disaster. The server load change requires an outage. Therefore, it is better to schedule this outage to occur in non-productions hours.

Returning to production entails the following high-level procedure:

1. Repair or recover the production N series storage system to its original state, with the correct software, options, and so on.
2. Copy the data (or changes) back to the production site from the disaster recovery site while the disaster recovery system is operational for users.
3. Prevent users or systems from accessing the disaster recovery data, and copy any final updates to production.
4. Split the mirror between the two sites.
5. Remap the production LUNs.
6. Rescan the VMware hosts, and inventory the virtual machines.
7. Start the virtual machines.
8. Re-establish SnapMirror from production to the disaster recovery site.

Because many of these steps are the same as in the disaster scenario, only the new steps are explained in detail in this section.

**FilerView versus CLI commands:** It is possible to perform some of the steps in this section and the following sections from FilerView. However, some are not available as they are not commonly performed operations. As a result, they are all shown as CLI commands.

## 12.5.1 Replicating data from disaster recovery to the production site

After the production site N series server becomes available, copy the data from the disaster recovery N series system to the production system. You can do this task by using one of the procedures in the following sections, depending on the state of the production N series data.

Before you begin, assign permissions in the reverse direction of what is explained in 12.3.3, “Setting permissions” on page 220, but enter the following command:

```
options snapmirror.access host=<secondary>
```

### Production N series data still intact

If the data in the production site was not lost, you need only to copy updates back from the disaster recovery site. You can perform this task by entering the following command:

```
snapmirror resync -S <DR_syste,m>:<volume> <prod_system>:<volume>
```

Example 12-3 shows the execution of the **snapmirror** command.

*Example 12-3 Synchronizing the production N series with disaster recovery updates*

```
itsotuc4>snapmirror resync -S 9.11.218.114:vol_vm_dest itsotuc4:vol_vm_source
The resync base Snapshot will be: itsotuc1(0118052508)_vol_vm_dest.5
Are you sure you want to resync the volume? yes
Thu May  1 23:30:55 MST last message repeated 2 times
Thu May  1 23:30:58 MST [itsotuc4: snapmirror.dst.resync.info:notice]: SnapMirror
resync of vol_vm_source to 9.11.218.114:vol_vm_dest is using
itsotuc1(0118052508)_vol_vm_dest.5 as the base Snapshot.
Volume vol_vm_source will be briefly unavailable before coming back online.
Thu May  1 23:30:59 MST [itsotuc4: wafl.snaprestore.revert:notice]: Reverting
volume vol_vm_source to a previous Snapshot.
Thu May  1 23:30:59 MST [itsotuc4: wafl.vol.guarantee.replica:info]: Space for
replica volume 'vol_vm_source' is not guaranteed.
Revert to resync base Snapshot was successful.
Thu May  1 23:30:59 MST [itsotuc4: snapmirror.dst.resync.success:notice]:
SnapMirror resync of vol_vm_source to 9.11.218.114:vol_vm_dest successful.
Transfer started.
Monitor progress with 'snapmirror status' or the snapmirror log.
itsotuc4>
```

### Production N series recovery

If the data in the production site was lost or corrupted during the disaster situation, you must re-create the volumes and then copy back all of the data from the disaster recovery site. You re-create the volume in the production site, and restrict the volume. Initialize the production system from the good copy on the disaster recovery system by entering the following command on the production N series system:

```
snapmirror initialize -S <dr_system>:<dr_vol> <prod_system>:<prod_vol>
```

Example 12-4 shows the **snapmirror initialize** command.

*Example 12-4 Copying the disaster recovery environment data to the production site*

```
itsotuc4> snapmirror initialize -S 9.11.218.114:vol_vm_dr itsotuc4:vol_vm_dr
Transfer started.
Monitor progress with 'snapmirror status' or the snapmirror log.
```

After the initialization is complete, the production system has a copy of the data again.

## 12.5.2 Preventing access and performing a final update

To ensure that the data is up to date, all virtual machines running on the disaster recovery site N series system must be shut down. Shutting down this system ensures that the final updates of data can be transferred back to the production system.

If a time lag exists between when the initialization was started and when it is convenient to schedule an outage on the guests, perform an update while the virtual machines are still running. Then shut down all guests that are accessing the disaster recovery site data.

When there is no longer anything accessing the DR site data, run the following command from the production N series system to perform the update:

```
snapmirror update -S <dr_system>:<dr_vol> <prod_system>:<prod_vol>
```

Example 12-5 shows the results of the **snapmirror update** command.

*Example 12-5 Updating data between the disaster recovery and production sites*

```
itsotuc4> snapmirror update -S 9.11.218.114:vol_vm_dr itsotuc4:vol_vm_dr
Transfer started.
Monitor progress with 'snapmirror status' or the snapmirror log.
itsotuc4>
```

## 12.5.3 Splitting the mirror

Now both the disaster recovery and production systems have the same data, and no changes are occurring on either system. Therefore, the mirror can be broken.

From the production N series system, quiesce and break the mirror by using the following command:

```
snapmirror break <volume_name>
```

Example 12-6 shows the execution of the **snapmirror break** command.

*Example 12-6 Breaking the mirror*

```
itsotuc4> snapmirror break vol_vm_dr
snapmirror break: Destination vol_vm_dr is now writable.
Volume size is being retained for potential snapmirror resync.  If you would like
to grow the volume and do not expect to resync, set vol option fs_size_fixed to
off.
itsotuc4>
```

### 12.5.4 Re-establishing the mirror from the production to disaster recovery site

Finally, you can perform a resynchronization to make the disaster recovery site a mirror of the production site again. Enter the following command on the disaster recovery N series system:

```
snapmirror resync <vol_name>
```

Example 12-7 shows the results of the **snapmirror resync** command.

*Example 12-7 Resync from the production to disaster recovery site*

```
itsotuc1> snapmirror resync vol_vm_dr
The resync base Snapshot will be: itsotuc4(0101165597)_vol_vm_dr.2
Are you sure you want to resync the volume? yes
Thu May  1 16:32:15 MST [snapmirror.dst.resync.info:notice]: SnapMirror resync of
vol_vm_dr to 9.11.218.238:vol_vm_dr is using itsotuc4(0101165597)_vol_vm_dr.2 as
the base Snapshot.
Volume vol_vm_dr will be briefly unavailable before coming back online.
Thu May  1 16:32:16 MST [wafl.snaprestore.revert:notice]: Reverting volume
vol_vm_dr to a previous Snapshot.
Thu May  1 16:32:16 MST [wafl.vol.guarantee.replica:info]: Space for replica
volume 'vol_vm_dr' is not guaranteed.
Revert to resync base Snapshot was successful.
Thu May  1 16:32:16 MST [snapmirror.dst.resync.success:notice]: SnapMirror resync
of vol_vm_dr to 9.11.218.238:vol_vm_dr successful.
Transfer started.
Monitor progress with 'snapmirror status' or the snapmirror log.
itsotuc1>
```

### 12.5.5 Configuring VMware hosts and virtual machines on the production site

Now the production N series system is the source again, and replication is occurring back to the disaster recovery site. Perform the following steps to start the guests on the production VMware hosts:

1. Rescan the VMware hosts to view the datastores again.

   The new datastore might be displayed as a snapshot. Therefore, you can rename it to the original name before using it, as in Figure 12-22.

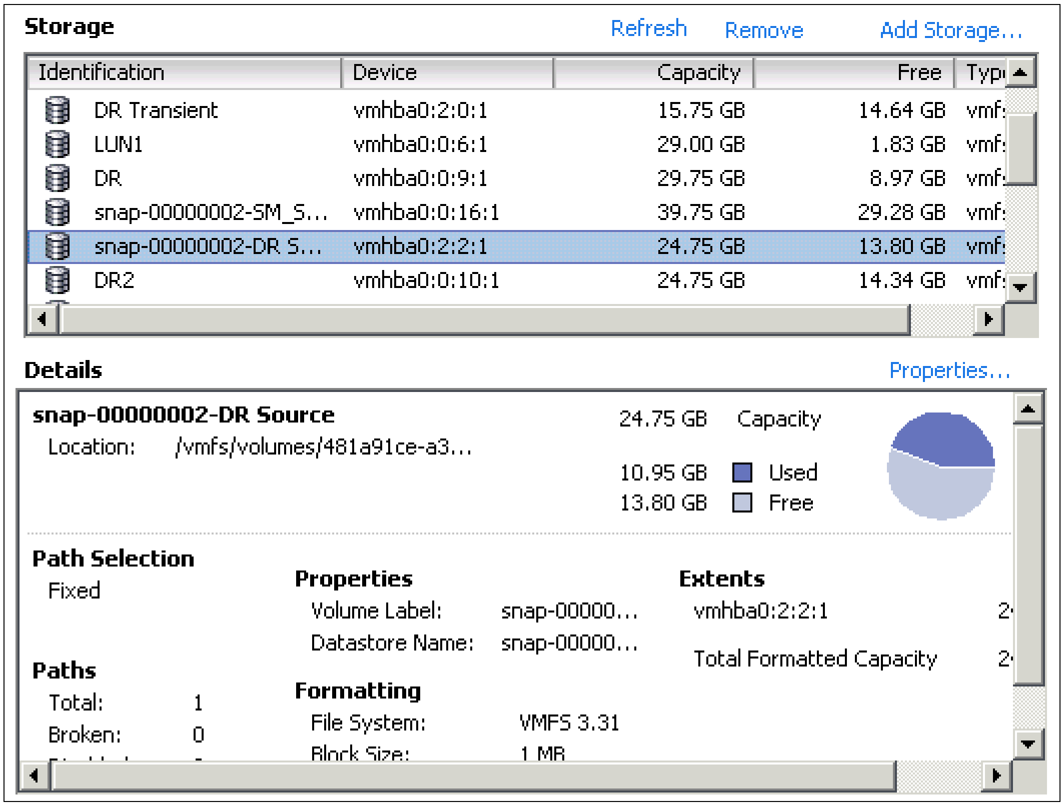



*Figure 12-22 Recovered datastore*

2. Reinventory the virtual machines.

   You might need to delete the original virtual machines first.

3. Reconfigure the virtual machines for the transient data volumes of the production site.
4. Start the virtual machines.

## 12.6 Disaster recovery testing

In a disaster recovery test, it is often desirable to perform testing without disrupting either the source environment or the destination copy of the data. Such a test is relatively easy to perform with the use of N series cloning, so that the disaster recovery environment can be tested against a clone of the mirrored data. Similar to other N series cloning processes, the clone requires little additional disk capacity in the disaster recovery site, because only changes are written to disk.

To perform this type of test, the LAN environment for the disaster recovery VMware hosts must be separated from the production environment. Thus, the guests can be started without causing conflicts in the network. You can complete this task by isolating the VMware hosts from the network (while still providing connectivity to the N series server). Alternatively, if feasible, you can set up isolated virtual networks within the VMware hosts. This second option, however, prevents communication between guests on separate hosts.

You can perform a disaster recovery test with N series cloning by using the following high-level procedure:

1. Verify that SnapMirror Snapshots in the disaster recovery location are current.
2. Clone the Snapshot volumes.
3. Bring the cloned LUNs online, and map them for access by the VMware hosts.
4. Rescan the VMware hosts.
5. Add the virtual machines to the inventory.
6. Start the virtual machines.
7. Perform disaster recovery application testing.
8. When complete, stop the virtual machines, remove them from the inventory, and destroy the cloned volumes.

# 13

# Deduplication with VMware vSphere 4.1

This chapter provides information about Advanced Single Instance Storage (A-SIS) deduplication and the benefits of enabling it. It also guides you step-by-step on how to set it up for a VMware vSphere 4.1 environment.

This chapter includes the following topics:

- A-SIS deduplication overview
- Storage consumption on virtualized environments
- When to run deduplication
- The effect of snapshots in deduplicated volumes
- Enabling deduplication on a volume

## 13.1 A-SIS deduplication overview

N series deduplication is a technology that can reduce the physical storage required to store a certain amount of data. Any typical data that might be stored in a disk volume has a certain amount of redundancy. It occurs in the form of identical data strings written to the volume multiple times. At a high level, the N series system can reduce the storage cost of this data. It does so by examining it and eliminating the inherent redundancies, as shown in Figure 13-1.

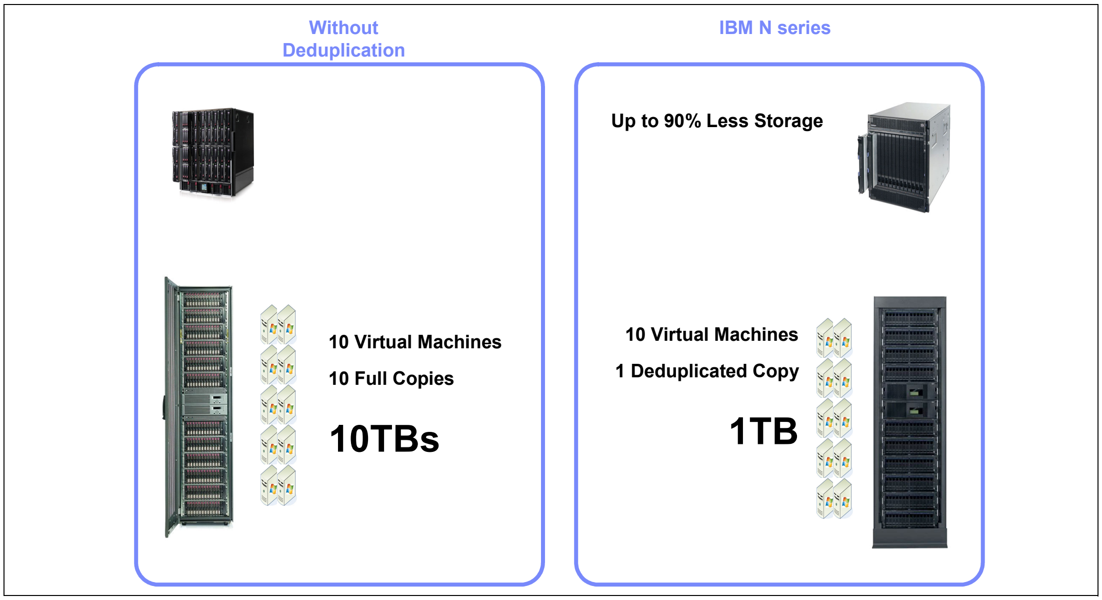



*Figure 13-1 A-SIS savings*

N series deduplication is managed at the volume level. Individual volumes can be configured to take advantage of deduplication, depending on the nature of the data in the volume. N series deduplication operates at the block level, which gives it a high level of granularity and efficiency. During the deduplication process, fingerprints of the individual blocks within a volume are compared to each other. When duplicate blocks are found, the system updates pointer files within the file system to reference one of the duplicate blocks. The others are deleted to reclaim free space.

The deduplication process does not occur at the time the data is written. It runs on a predetermined schedule or can be started manually at any time. Because deduplication process can be run at any time after the data was written, the performance impact of deduplication is low. During times when the storage system is busy or is accepting many new write operations, the only impact is the lightweight fingerprinting process. The total impact to performance of the system is low. The more I/O intensive deduplication process can then be scheduled to run during a period of low activity.

The amount of space savings using deduplication vary depending on the nature of the data being deduplicated. Results of anywhere between 10% and 90% space savings can be seen, but 50% or more is common.

## 13.2 Storage consumption on virtualized environments

Although any type of data can be effectively deduplicated by N series deduplication, the data on virtualized environment has several unique characteristics that make deduplication effective. For example, when a virtual disk is created, a file equal to the size of the virtual disk is created in a datastore. This virtual disk file consumes space equal to its size regardless of how much data is stored in the virtual disk. Any allocated but unused space (sometimes called *white space*) is identical redundant space on the disk and a prime candidate for deduplication.

Another unique characteristic of that data is related to the way that virtual machines are created. A common deployment method is to create templates and then deploy new virtual machines by cloning the template. The result is virtual machines that have a high level of similarity in their data.

In a traditional deployment, each new virtual machine takes new storage. Here, N series deduplication can help to reduce the amount of storage required to store the virtual machine images. When two or more virtual machines are stored in the same datastore, any common data between them can be duplicated. (The common data includes operating system binary files, application binary files, and free space.) In some cases, that data can be deduplicated down to the equivalent of a single copy it.

## 13.3 When to run deduplication

As mentioned previously, the N series deduplication process does not occur at the time that the data is written to the storage device. However, it can be run any time the administrator desires after the data was written. The deduplication process can be resource-intensive, and it is best to run it during a period of low activity.

You can schedule and start the deduplication process using one of several ways. For example, the process can be started automatically on a fixed schedule. It can be started automatically after a defined amount of new data was written to the volume (20% by default). Alternatively, you can start it manually at anytime. Run the deduplication process manually when a significant amount of data must be deduplicated. For example, run it after provisioning new virtual machines.

## 13.4 The effect of snapshots in deduplicated volumes

Although snapshots can be used in deduplicated volumes, you must take note of one operational difference. The deduplication process can identify and deduplicate redundant blocks that are in a snapshot. However, the block reclamation process cannot return to blocks to free space while the snapshots exist. Because of this behavior, you might experience lower than expected space savings when deduplicating data in a volume that has snapshots.

When all of the snapshots that were taken before the deduplication process are deleted, the deduplicated blocks are reclaimed as free space. As a result of this behavior, you might want to deduplicate new data before any snapshots are taken. However, it might not always be practical, especially in busy environments.

## 13.5 Enabling deduplication on a volume

This section explains how to set up deduplication on an N series for use with VMware servers. It also provides information about storage reduction after enabling it for Network File System (NFS) and Fibre Channel Protocol (FCP) volumes.

## 13.5.1 Setting up deduplication on a volume

In this section, you go step-by-step through the process to set up deduplication. This scenario is based on the creation of five identical guests of 10 GB each on the NFS and FCP. For more information about how to set up FCP LUNs and NFS for ESX, see 5.3, “Preparing N series for the VMware ESXi Server” on page 63. The size for the FCP LUN and the NFS share is 50 GB each.

### The deduplication process

Figure 13-2 shows the original sizes of the NFS share as viewed through ESX server management console.

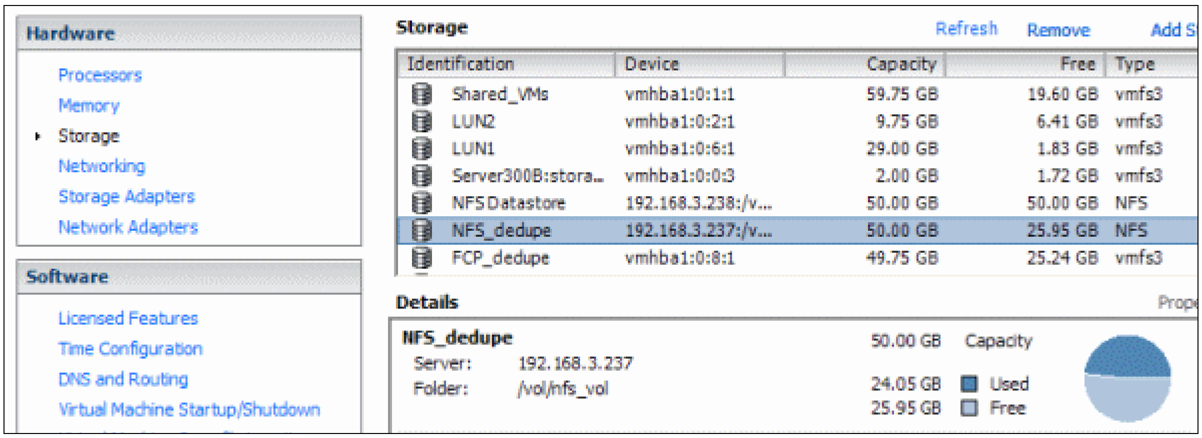



*Figure 13-2 NFS size on the vCenter management console before deduplication*

Figure 13-3 shows the original sizes of the FCP LUN as viewed through the ESX server management console.

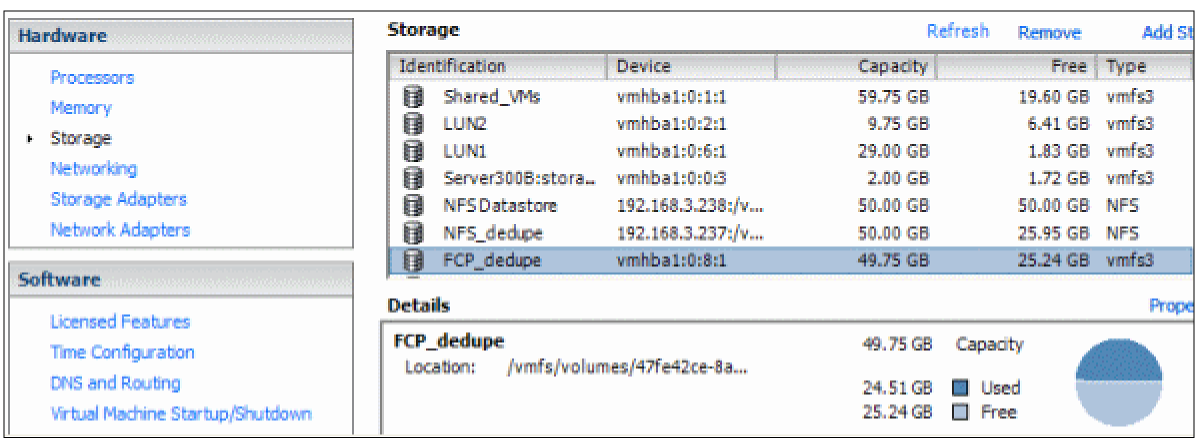



*Figure 13-3 FCP size on vCenter management console before deduplication*

Example 13-1 shows the size of the NFS share as viewed on the N series command line.

*Example 13-1 NFS size on the N series CLI*

```
itsotuc3> df -g /vol/nfs_vol
Filesystem               total      used      avail  capacity  Mounted on
/vol/nfs_vol/            50GB       24GB      25GB       48%   /vol/nfs_vol/
/vol/nfs_vol/.snapshot    0GB        0GB       0GB      ---%   /vol/nfs_vol/.
snapshot
```

Example 13-2 shows the size of the FCP LUN as viewed on the N series command line.

*Example 13-2 LUN size on the N series CLI*

```
itsotuc3> df -g /vol/fcp_vol
Filesystem               total      used      avail  capacity  Mounted on
/vol/fcp_vol/             60GB      50GB      9GB         84%   /vol/fcp_vol/
/vol/fcp_vol/.snapshot     0GB       0GB      0GB        ---%   /vol/fcp_vol/.
snapshot
```

To enable deduplication on a volume, enter the **sis on <vol_name>** command as follows:

- For an NFS volume, enter the command as shown in Example 13-3.

  *Example 13-3 Enabling deduplication*

  ```
  itsotuc3> sis on /vol/nfs_vol
  SIS for "/vol/nfs_vol" is enabled.
  Already existing data could be processed by running "sis start -s
  /vol/nfs_vol".
  itsotuc3>
  ```

- For an FCP volume, follow these steps:

  a. Set the fractional reserve to 0 (Example 13-4).

  *Example 13-4 Setting the fractional reserve*

  ```
  itsotuc3> vol options fcp_vol fractional_reserve 0
  ```

  b. Enable deduplication on the FCP volume (Example 13-5).

  *Example 13-5 Enabling deduplication on the FCP volume*

  ```
  itsotuc3> sis on /vol/fcp_vol
  SIS for "/vol/fcp_vol/" is enabled.
  Already existing data could be processed by running "sis start -s
  /vol/fcp_vol".
  ```

  c. Check the status (Example 13-6).

  *Example 13-6 Checking the status*

  ```
  itsotuc3> sis status
  Path                            State      Status      Progress
  /vol/fcp_vol                    Enabled    Active      670 MB Scanned
  /vol/nfs_vol                    Enabled    Active      9497 MB Scanned
  ```

### Deduplicating existing data

You can start the deduplication process at any time by using the **sis start <vol>** command. The default behavior of the command deduplicates only data that was written since deduplication was turned on for the volume.

To deduplicate data that was written before deduplication was enabled, use the **sis start -s <vol>** command.

To start the deduplication process, use the **sis start -s <vol_name>** command (Example 13-7).

*Example 13-7 Starting the deduplication process*

```
itsotuc3> sis start -s /vol/nfs_vol
The file system will be scanned to process existing data in /vol/nfs_vol.
This operation may initialize related existing metafiles.
Are you sure you want to proceed with scan (y/n)?y
Starting SIS volume scan on volume nfs_vol.
The SIS operation for "/vol/nfs_vol" is started
```

Example 13-8 shows how to start the deduplication process on a SAN volume.

*Example 13-8 Starting the deduplication process on a SAN volume*

```
itsotuc3> sis start -s /vol/fcp_vol
The file system will be scanned to process existing data in /vol/fcp_vol.
This operation may initialize related existing metafiles.
Are you sure you want to proceed with scan (y/n)?y
Starting SIS volume scan on volume fcp_vol.
The SIS operation for "/vol/fcp_vol" is started.
```

## 13.5.2 Deduplication results

To check the progress of the deduplication process, use the **sis status** command, as shown in Example 13-9. If the status is `active`, the process of deduplication is still on going. If the status is `idle`, deduplication is completed.

*Example 13-9 Checking status*

```
itsotuc3> sis status
Path                            State      Status      Progress
/vol/fcp_vol                    Enabled    Idle        Idle for 02.18.36
/vol/nfs_vol                    Enabled    Idle        Idle for 02:12:50
```

When the process is completed, you can view the space savings from the Virtual Infrastructure client or on the storage controller. Use the **df -s** command (Example 13-10).

*Example 13-10 N series node*

```
itsotuc3> df -gs /vol/nfs_vol
Filesystem                used      saved      %saved
/vol/nfs_vol               2GB       21GB         91%
```

The space savings of NFS volumes are available immediately and can be observed from both the storage controller and Virtual Infrastructure Client. The NFS example (Example 13-10) starts with a total of 24 GB, which is reduced to 2 GB for a total savings of 91%.

The savings displayed on the N series node match what is shown on the ESX management console. In Figure 13-4, in the highlighted area, now 47.71 GB of space is available on the NFS share.

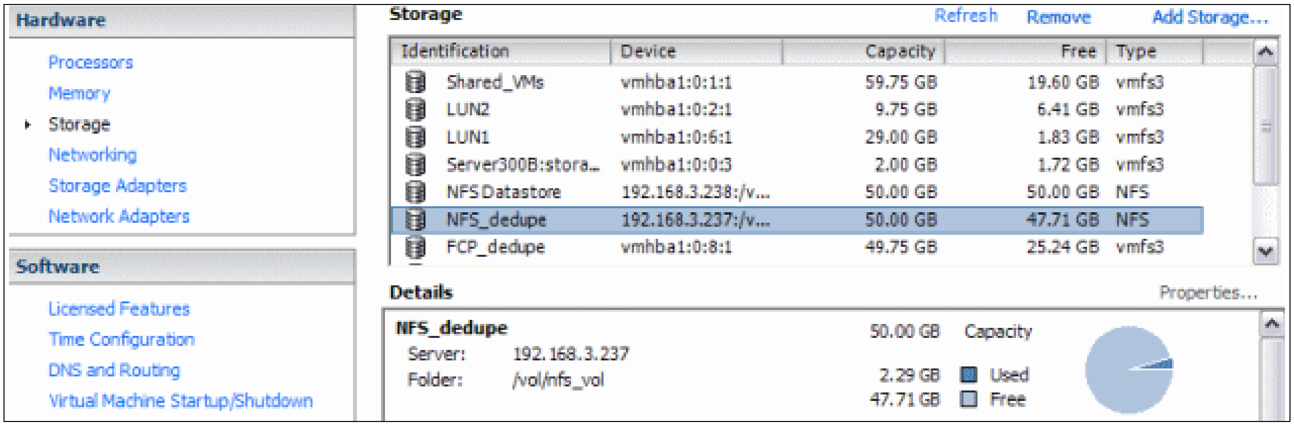



*Figure 13-4 Savings display*

## 13.5.3 Deduplication of LUNs

Deduplication is effective on VMFS datastores and LUNs. However, as default behavior, a LUN on the N series storage system reserves space in the volume equal to the size of a LUN. Deduplication cannot reduce this reservation. Although it is enabled, there is no way to realize the space savings of deduplication on the LUN. To realize the space savings, the space reservation of the LUN must be disabled. This option is set on each LUN individually and can be set in the GUI or by using the **`lun set reservation`** command.

> **Space allocation on the VMFS file system:** Deduplication reduces the amount of physical storage that the LUN consumes on the storage device. However, it does not change the logical allocation of space within the VMFS file system. This situation is unlike an NFS datastore, where space savings are realized immediately and new data can be written to the datastore. For VMFS file systems, deduplication cannot change the total amount of space that can be stored in a VMFS datastore.

After deduplication is complete, you can use the free space gained to store new data. You can create a LUN in the same volume and connect it as a new datastore. Alternatively, you can shrink the existing volume and use the space saved to grow other volumes or create new volumes.

To disable space reservation for the LUN, run the **lun set reservation <lun_path>** command (Example 13-11).

*Example 13-11 Setting LUN reservation*

```
itsotuc3> lun set reservation /vol/fcp_vol/deduplication disable
```

Now you can see the storage savings on the volume that contains the LUN deduplication (Example 13-12).

*Example 13-12 Storage savings displayed*

```
itsotuc3> df -gs /vol/fcp_vol
Filesystem                used      saved      %saved
/vol/fcp_vol/              20%       21GB          91%
```

Unlike NFS, the FCP savings are not apparent when you verify the VMware vCenter management console.

14

# Virtual Storage Console

The ability to quickly back up tens of hundreds of virtual machines without affecting production operations can accelerate the adoption of VMware within an organization.

The Virtual Storage Console (VSC) feature was formerly provided in a separate interface and was called SnapManager for Virtual Infrastructure (SMVI). It builds on the N series SnapManager portfolio by providing array-based backups. These consume only block-level changes to each VM and can provide multiple recovery points throughout the day. The backups are an integrated component within the storage array. Therefore, VSC provides recovery times that are faster than times provided by any other means.

## 14.1 Introduction to the Virtual Storage Console

The Virtual Storage Console (VSC) software is a single vCenter Server plug-in. It provides end-to-end virtual machine lifecycle management for VMware environments running N series storage. The plug-in provides these features:

- Storage configuration and monitoring, using the Monitoring and Host Configuration capability (previously called the Virtual Storage Console capability)
- Datastore provisioning and virtual machine cloning, using the Provisioning and Cloning capability
- Backup and recovery of virtual machines and datastores, using the Backup and Recovery capability

As a vCenter Server plug-in, shown in Figure 14-1, the VSC is available to all vSphere Clients that connect to the vCenter Server. This availability is different from a client-side plug-in that must be installed on every vSphere Client. You can install the VSC software on a Windows server in your data center, but you must not install it on a client computer.

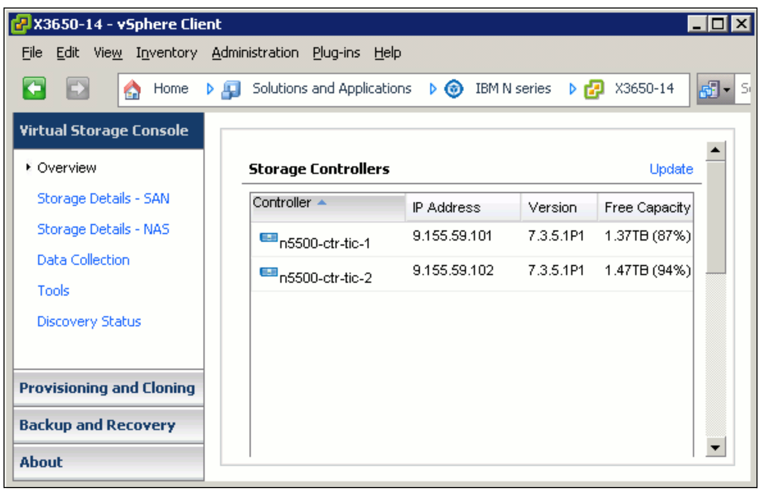



*Figure 14-1 Virtual Storage Console 2*

Virtual Storage Console (VSC) integrates VSC storage discovery, health monitoring, capacity management, and best practice-based storage setting. It offers additional management capabilities with two capability options in a single vSphere™ client plug-in. Thus it enables centralized, end-to-end management of virtual server and desktop environments running on N series storage. VSC is composed of three main components:

- Virtual Storage Console Capability (base product): Provides a storage view of the VMware® environment with a VM administrator perspective. It automatically optimizes the customer’s host and storage configurations, including HBA timeouts, NFS tunables, and multipath configurations. Using the Virtual Storage Console, a VM administrator can quickly and easily view controller status and capacity information. Also, the administrator can accurately report back utilization information in order to make more informed decisions about VM object placement.
- Provisioning and Cloning Capability: Provides end-to-end datastore management (provisioning, resizing, and deletion). Also offers rapid, space-efficient VM server and desktop cloning, patching, and updating by using FlexClone® technology.

- Backup and Recovery capability (formerly SnapManager® for Virtual Infrastructure): Automates data protection processes by enabling VMware administrators to centrally manage backup and recovery of datastores and VMs. This can be done without impacting guest performance. The administrator can also rapidly recover from these backup copies at any level of granularity: datastore, VM, VMDK, or guest file.

VSC is designed to simplify storage management operations, improve efficiencies, enhance availability, and reduce storage costs in both SAN- and NAS-based VMware infrastructures. It provides VMware administrators with a window into the storage domain. It also provides the tools to effectively and efficiently manage the lifecycle of virtual server and desktop environments running on N series storage.

## 14.1.1 License requirements

Table 14-1 summarizes the N series license requirements to perform different VSC functions.

*Table 14-1 VSC license requirements*

| Task | License |
|---|---|
| Provision datastores | NFS, FCP, iSCSI |
| Restore datastores | SnapRestore |
| Use vFilers in Provisioning and Cloning operations | MultiStore |
| Clone virtual machines | FlexClone (NFS only) |
| Configure deduplication settings | A-SIS |
| Distribute templates to remote vCenters | SnapMirror |

## 14.1.2 Architecture overview

Figure 14-2 illustrates the architecture for VSC. It also shows the components that work together to provide a comprehensive and powerful backup and recovery solution for VMware vSphere environments.

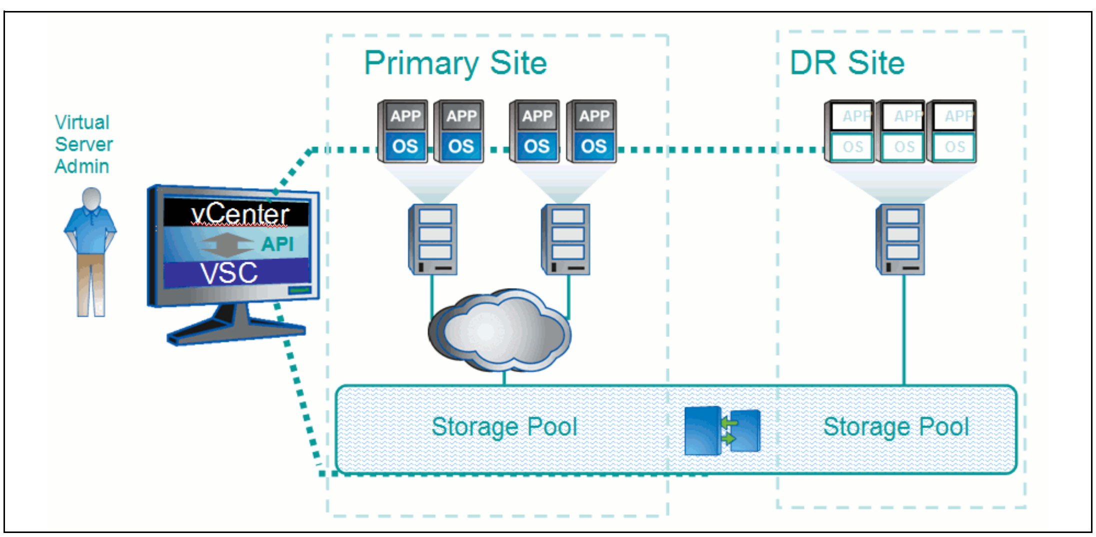



*Figure 14-2 Architecture overview*

## 14.1.3 Monitoring and host configuration

The Monitoring and Host Configuration capability enables you to manage ESX and ESXi servers connected to N series storage systems. You can set host timeout, NAS, and multipathing values, view storage details, and collect diagnostic data. You can use this capability to do the following tasks:

- View the status of storage controllers from a SAN (FC, FCoE, and iSCSI) perspective
- View the status of storage controllers from a NAS (NFS) perspective
- View SAN and NAS datastore capacity utilization
- View the status of VMware vStorage APIs for Array Integration (VAAI) support in the storage controller
- View the status of ESX hosts, including ESX version and overall status
- Check at a glance whether the following settings are configured correctly, and if not, automatically set the correct values:
  - Storage adapter timeouts
  - Multipathing settings
  - NFS settings
- Set credentials to access storage controllers
- Launch the FilerView GUI to create LUNs and manage storage controllers
- Collect diagnostic information from the ESX hosts, storage controllers, and Fibre Channel switches
- Access tools to set guest operating system timeouts and to identify and correct misaligned disk partitions

When you click the N series icon in the vCenter Server and click Monitoring and Host Configuration in the navigation pane, the Overview panel displays. It is similar to Figure 14-3.

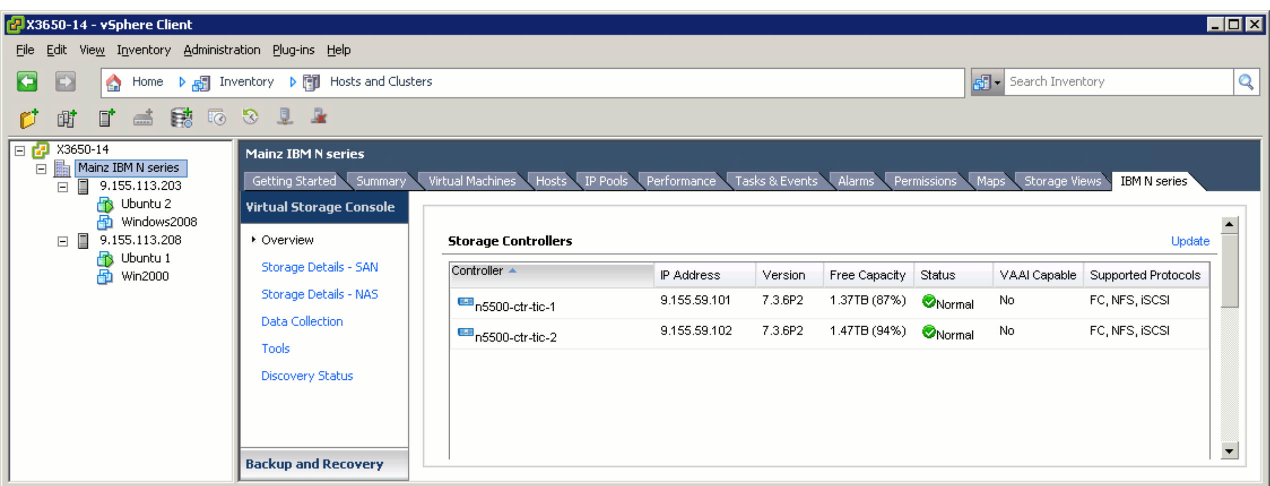



*Figure 14-3 VSC overview*

Alternatively, you can find the VSC plug-in under Solutions and Applications (Figure 14-4).

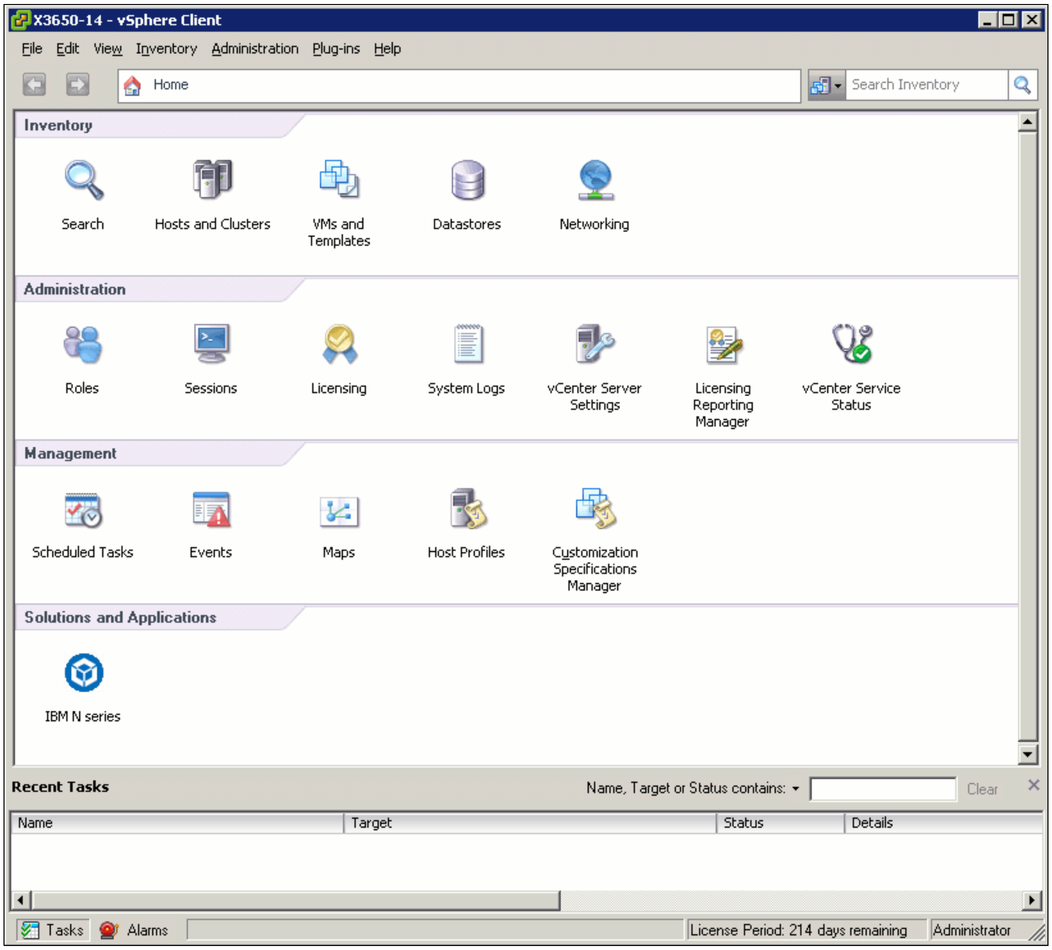



*Figure 14-4 VSC location*

## 14.1.4 Provisioning and Cloning

The Provisioning and Cloning capability of Virtual Storage Console helps you to provision datastores and quickly create multiple clones of virtual machines in the VMware environment. Using FlexClone technology, the Provisioning and Cloning capability allows you to efficiently create, deploy, and manage the lifecycle of virtual machines. These tasks can be done from an easy-to-use interface integrated into the VMware environment. It is ideal for virtual server, desktop, and cloud environments. You can use this capability for the following purposes:

- Clone individual virtual machines and place in new or existing datastores
- Create, resize, or delete datastores
- Apply guest customization specifications and power up new virtual machines
- Run deduplication operations
- Monitor storage savings
- Redeploy virtual machines from a baseline image
- Replicate NFS datastores across sites
- Import virtual machines into virtual desktop infrastructure connection brokers and management tools

## Managing datastores and cloning virtual machines

To manage datastores and clone virtual machines, right-click an object in the Inventory panel of the vSphere Client and select **N series** → **Provisioning and Cloning**:

- Right-click a powered-down virtual machine or template to create clones.
- Right-click a datacenter, cluster, or host to provision datastores.

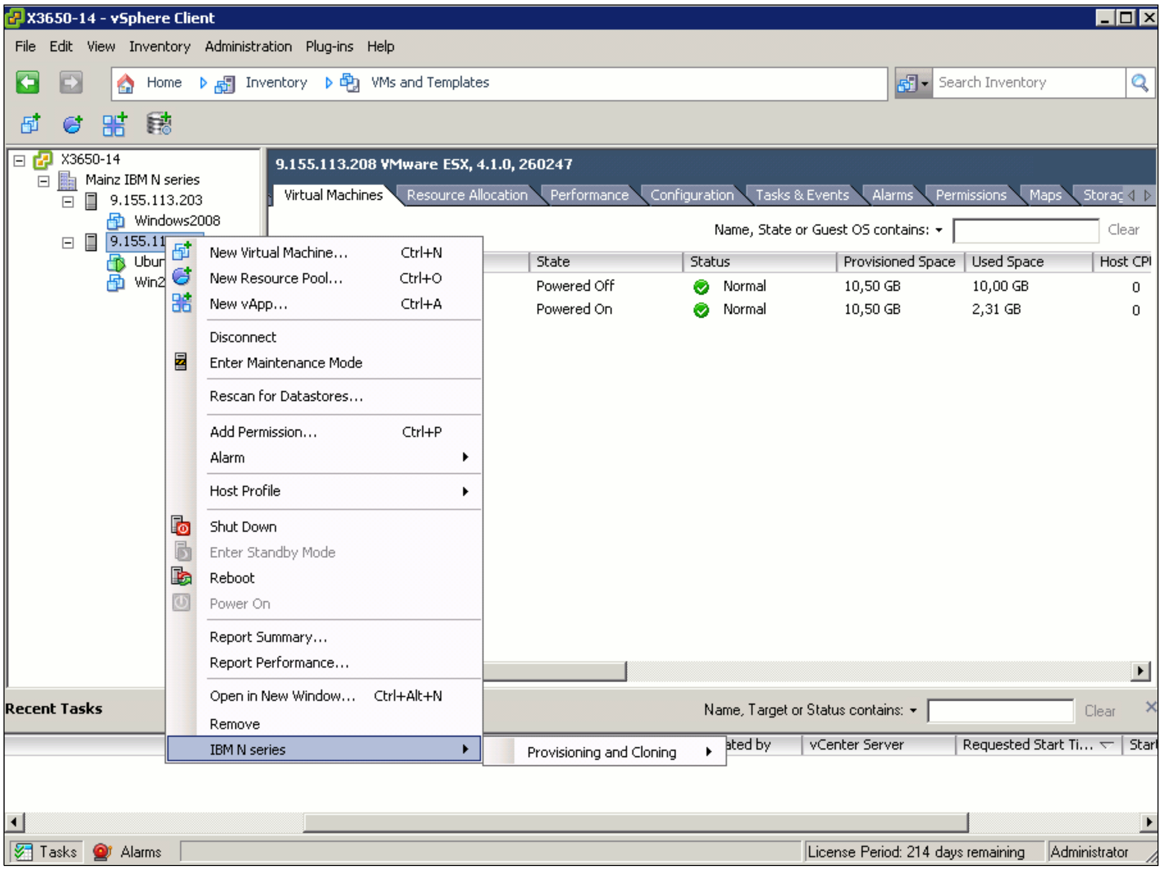



*Figure 14-5 Accessing Provisioning and Cloning*

## Managing controllers, replicating datastores, and redeploying clones

Click the Inventory button in the navigation bar, and then select **Solutions and Applications** → **N series**. Use the following options:

- Select **Storage controllers** to add, remove, or modify properties of storage controllers.
- Select **Connection brokers** to add and remove connection broker definitions.
- Select **DS Remote Replication** to clone NFS datastore templates to multiple target sites.
- Select **Redeploy** to redeploy virtual machines.

# 14.2 Installing the Virtual Storage Console 2.0

The VSC provides full support for hosts running ESX/ESXi 4.0 and later. It provides limited reporting functionality with hosts running ESX/ESXi 3.5 and later.

## 14.2.1 Basic installation

Before downloading and installing the VSC, make sure that your deployment has the required components:

- You need a vCenter Server version 4.0 or later. The VSC can be installed on the vCenter Server or on another server or VM (see Figure 14-6).
- If installing on another server or VM, this system must run 32-bit or 64-bit Windows Server 2008, 2003 SP1 and later, or a 32-bit version of XP Professional SP2 and later.
- A storage array is required to run Data ONTAP 7.3.1.1 or later.

**Attention:** Before installing, verify supported storage adapters and firmware.

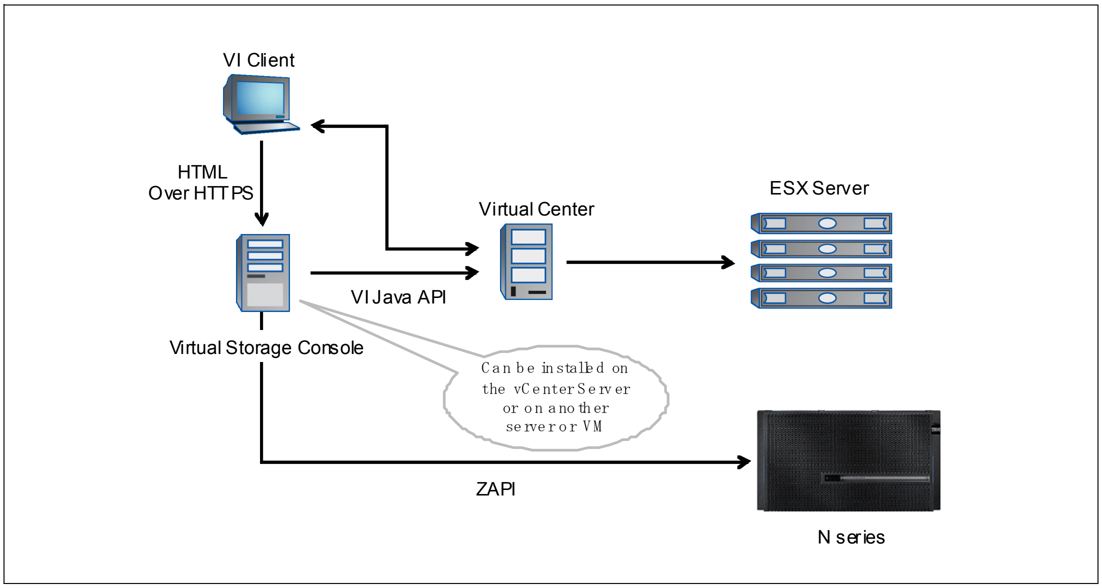



*Figure 14-6 VSC possible deployments*

**Tip:** To keep it simple, we suggest installing the VSC on the vCenter server.

Complete the following steps to install the VSC 2.0:

1. Download the installation program to the Windows server.
2. Run the installation wizard and select the features you would like to install as shown in Figure 14-7.
3. Follow the on-screen instructions.

   During the installation process, a prompt displays to select the features of the VSC 2.0 to be enabled in the environment. The core VSC must be selected. The Provisioning and Cloning and Backup and Recovery features are the former RCU and the SMVI interfaces. Certain subfeatures might require licensing, as described previously.

4. Register the VSC as a plug-in, in the vCenter Server in the window that opens when the process is complete.

   This final step requires a user with vCenter administrator credentials to complete the registration process.

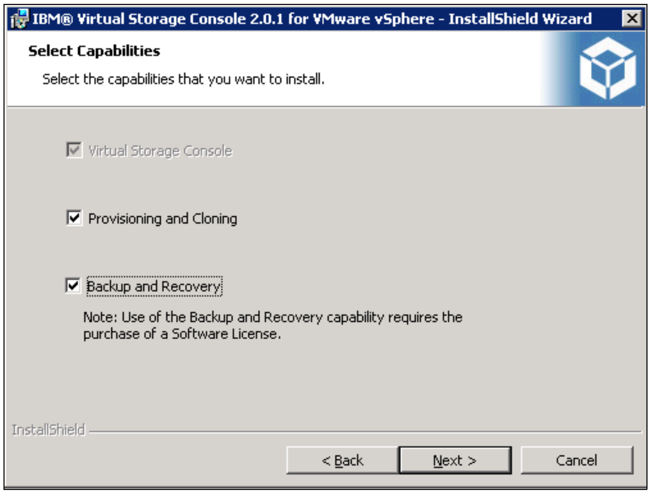



*Figure 14-7 Select VSC features*

The installation process launches the vCenter registration process as shown in Figure 14-8.

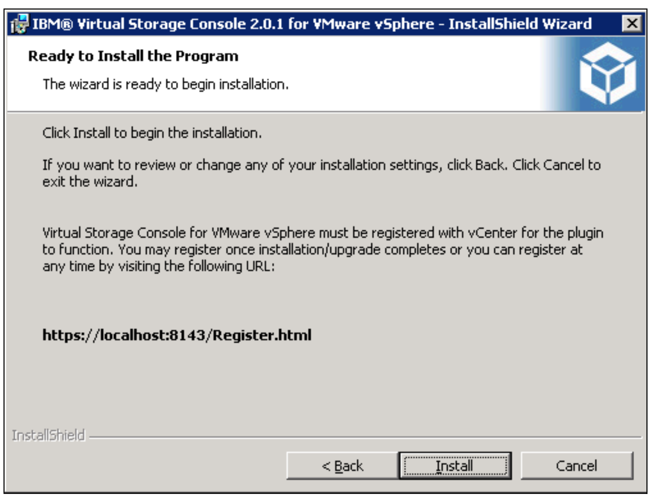



*Figure 14-8 vCenter registration process*

5. Finally, register the VSC plug-in with a vCenter server (Figure 14-9).

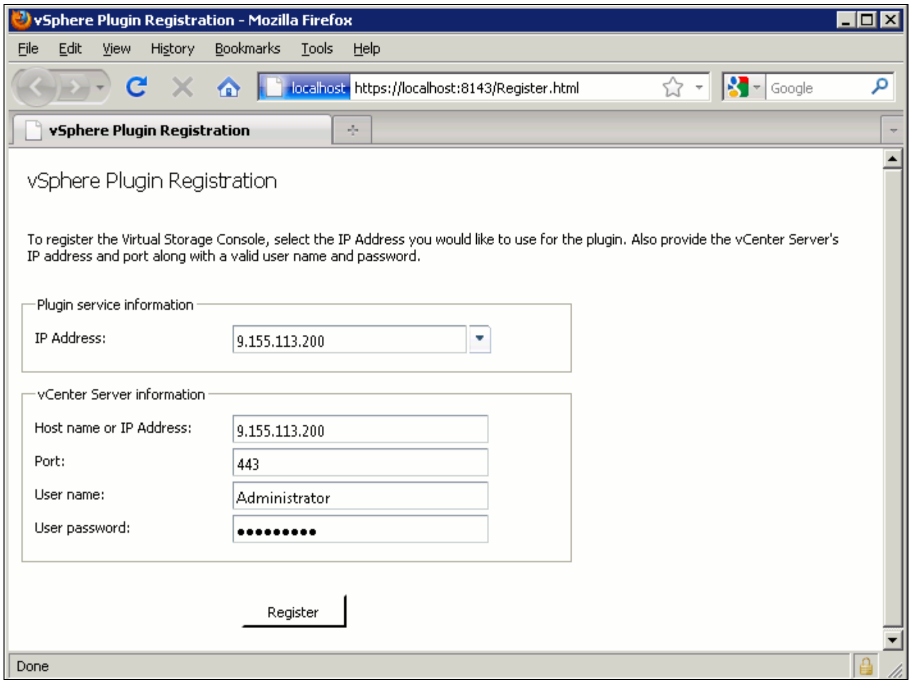



*Figure 14-9 VSC registration with vCenter server*

Upon successful registration, the system confirms by issuing the following message on the web page: `The registration process has completed successfully!`

## 14.2.2 Upgrading the VSC

As of December 2011, an upgrade to VSC 2.1.1 is available that needs to be installed after installing and registering VSC2.0 (see Figure 14-10). Follow these steps:

1. Download the installer for VSC.
2. Double-click the installer icon, and click **Run** to start the installation wizard.
3. Click **Yes** on the confirmation prompt.
4. In the installation wizard, select the capabilities that you want to upgrade and click **Next** to start the installation. The installation might take several minutes.
5. Click **Finish** to complete the installation.

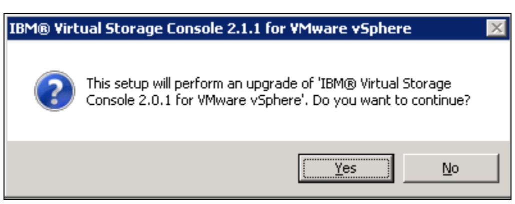



*Figure 14-10 Upgrade to VSC 2.1.1*

**Support:** VSC 2.1.1 supports upgrades from VSC 2.0 only. The VSC installer does not support upgrades from a version of VSC prior to 2.0 or from stand-alone versions of RCU or VSC (SMVI). If you have that software installed, you must uninstall it before you can install VSC 2.1.1. If the VSC installer finds one of those versions of VSC, RCU, or SMVI on the server, it prompts you to uninstall the software. Then the installer aborts.

The VSC installer checks the version numbers of each of the currently installed capabilities as shown in Figure 14-11. It lets you upgrade each capability that has an older version number than the one you are installing.

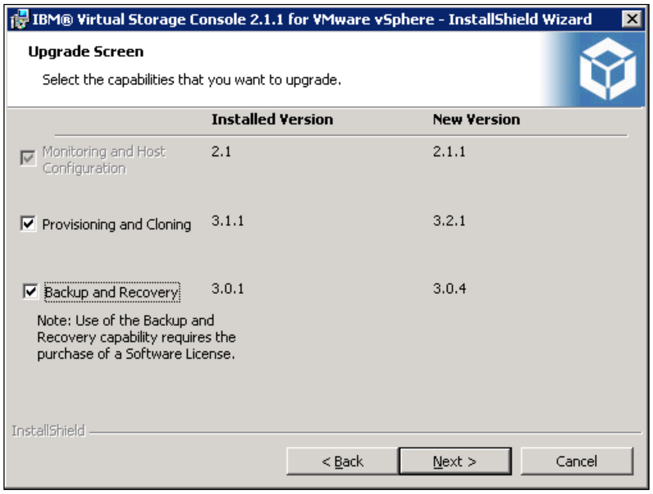



*Figure 14-11 Select VSC upgrades*

6. A web page displays when the installation is complete. You must register VSC with the vCenter Server. You must provide the vCenter Server host name or IP address and the administrative credentials.

**Attention:** After you finish, you must close the vSphere Client and restart it to display newly installed capabilities.

# 14.3 Adding storage controllers to the VSC

Adding the storage controllers that host the virtual infrastructure to the VSC is fairly simple:

1. Connect to vCenter by using the vSphere client.
2. Double-click the N series icon on the Home panel.
3. Select the Virtual Storage Console tab on the left.

After these steps are completed, the VSC launches and automatically identifies all storage controllers powered by Data ONTAP with the storage connected to the ESX/ESXi hosts in the environment. As an alternative to running discovery for the entire environment, you can select an ESX/ESXi host or cluster in the vSphere client and then select the NetApp tab in the left panel. The VSC then begins discovery of all storage controllers with storage connected to the host or cluster that was selected.

The Controller Credentials wizard starts, displayed in Figure 14-12, allowing you to enter the user or service account assigned for VSC management on the storage controller. This account can be the root account or one created specifically for the VSC core feature, as described previously.

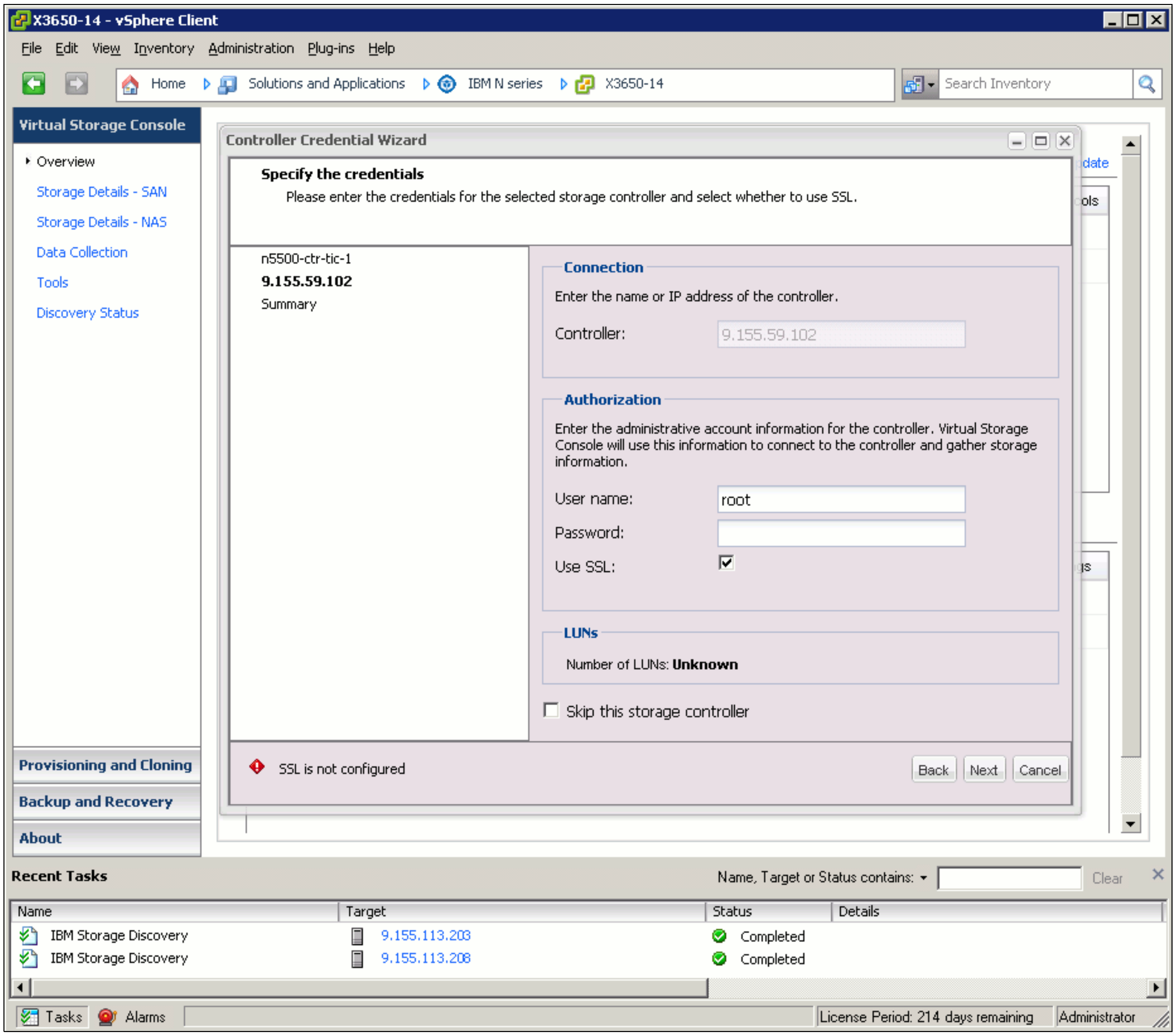



*Figure 14-12 Adding storage controller access in VSC*

## 14.4 Optimal storage settings for ESX/ESXi hosts

The VSC enables the automated configuration of storage-related settings for all ESX/ESXi 4.x hosts connected to NetApp storage controllers. VMware administrators can right-click individual or multiple ESX/ESXi hosts and set the preferred values for these hosts. This functionality sets values for HBAs and CNAs, sets appropriate paths and path selection plug-ins, and provides appropriate settings for software-based I/O (NFS and iSCSI).

To perform the setting, go to the VSC pane, right-click the designated ESX server, and run the settings as shown in Figure 14-13.

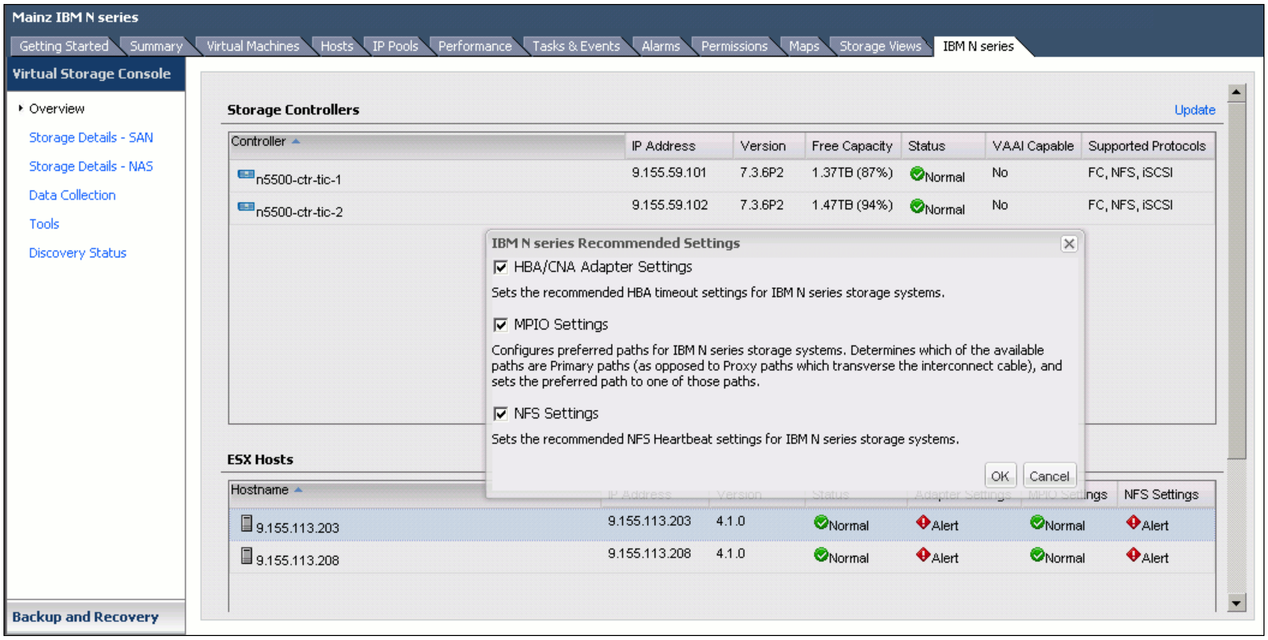



*Figure 14-13 Optimize ESX settings*

After rebooting the ESX server, we can verify the improved settings. All status indicators are green (see Figure 14-14).

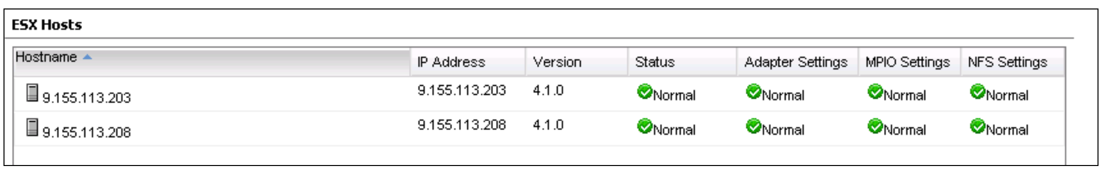



*Figure 14-14 Optimized ESX adapter settings*

# 14.5 SnapMirror integration

SnapMirror relationships cannot be configured through VSC. However, VSC can update an existing SnapMirror relationship on the volume underlying the datastore or virtual machine. Preferably, test the SnapMirror relationship from the storage system command line before updating through VSC. This method aids in identifying where any potential issues might occur. If the SnapMirror update is successful from the CLI, but fails from within VSC, the administrator has a better understanding of where to concentrate troubleshooting efforts.

Also, identify the destination storage within VSC in the same manner that the relationship is configured on the storage system. For example, if a SnapMirror relationship is configured on the storage system using IP addresses rather than a DNS name, identify the auxiliary storage to VSC by the IP address and vice versa.

Because its support is for SnapMirror volume only, map one volume per datastore.

During backup creation, SnapManager provides the option of updating an existing SnapMirror relationship. That way, every time a Snapshot is created, the data is transferred to a remote storage system. Whenever the backup of a virtual machine or datastore is initiated with the SnapMirror option, the update starts as soon as the backup completes, after of the current SnapMirror schedule.

For example, by configuring regular SnapMirror updates on a filter after the VSC schedule, you can cut down the time required to update the mirror, because it is done in the interim. However, keep in mind that the updates must be scheduled in such a way that they do not conflict with the SnapManager backup.

### 14.5.1 SnapMirror destinations

A single SnapMirror destination is supported per volume. If a SnapMirror update is selected as part of a backup on a volume with multiple destinations, the backup fails.

If multiple SnapMirror destinations are required, use a tiered approach when configuring the SnapMirror relationships. For example, if the data must be transferred to four destinations, configure one destination from the primary storage system supported to one destination. Then configure three additional destinations from the auxiliary storage through the storage system CLI.

### 14.5.2 SnapMirror and deduplication

Preferably, do not use deduplication with Sync SnapMirror. Although technically it works, the integration and scheduling of deduplication with Sync SnapMirror are complicated to implement in the type of rigorous real-world scenarios that demand synchronous replication.

When configuring volume SnapMirror and deduplication, consider the deduplication schedule and the volume SnapMirror schedule. Start volume SnapMirror transfers of a deduplicated volume after deduplication completes (that is, not during the deduplication process). This technique avoids sending undeduplicated data and additional temporary metadata files over the network. If the temporary metadata files in the source volume are locked in Snapshot copies, they also consume extra space in the source and destination volumes. Volume SnapMirror performance degradation can increase with deduplicated volumes.

The scenario described previously has a direct impact on backups configured within VSC when the SnapMirror update option was selected. Avoid scheduling a backup with the SnapMirror update option until a a confirmation of the volume deduplication completeness. Although a few hours must be scheduled to ensure avoiding this issue, the actual scheduling configuration is data and customer dependent.

## 14.6 VSC in an N series MetroCluster environment

N series MetroCluster configurations consist of a pair of active-active storage controllers. They are configured with mirrored aggregates and extended distance capabilities to create a high-availability solution. This type of configuration has the following benefits:

- Higher availability with geographic protection
- Minimal risk of lost data, easier management and recovery, and reduced system downtime
- Quicker recovery when a disaster occurs
- Minimal disruption to users and client applications

A MetroCluster (either Stretch or Fabric) behaves in most ways similar to an active-active configuration. All of the protection provided by core N series technology (RAID-DP, Snapshot copies, automatic controller failover) also exists in a MetroCluster configuration. However, MetroCluster adds complete synchronous mirroring along with the ability to perform a complete site failover from a storage perspective with a single command.

The following N series MetroCluster types exist and work seamlessly with the complete VMware vSphere and ESX server portfolio:

- *Stretch MetroCluster* (sometimes called a *nonswitched cluster*) is an active-active configuration that can extend up to 500 m depending on speed and cable type. It includes synchronous mirroring (SyncMirror) and the ability to do a site failover with a single command.
- *Fabric MetroCluster* (also called a *switched cluster*) uses four Fibre Channel switches in a dual-fabric configuration. It uses a separate cluster interconnect card to achieve an even greater distance (up to 100 km depending on speed and cable type) between primary and secondary locations.

The integration of the MetroCluster and VMware vSphere is seamless and provides storage and application redundancy. In addition to connecting to the vSphere environment using FCP, iSCSI, or NFS, this solution can serve other network clients with CIFS, HTTP, and FTP at the same time. The solution shown in Figure 14-15 provides a redundant VMware server, redundant N series heads, and redundant storage.

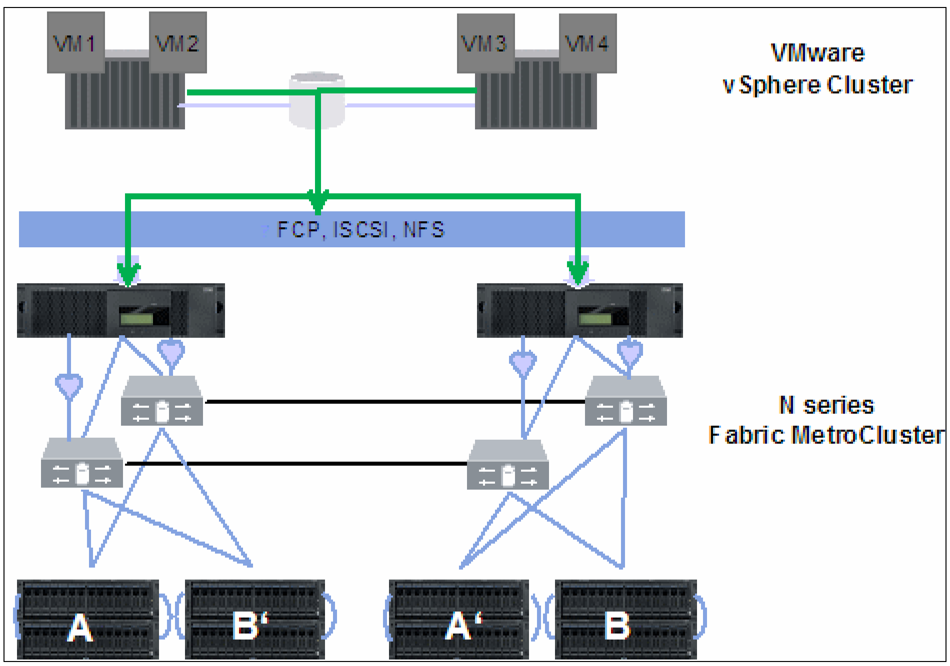



*Figure 14-15 MetroCluster and VMware vSphere integrated solution*

For more information about N series MetroCluster, see the “MetroCluster” chapter in the Redbooks publication, *IBM System Storage N series Software Guide*, SG24-7129.

## 14.7 Backup and recovery

This section provides examples of backing up a single virtual machine or the entire DataCenter. The Backup and Recovery capability of the Virtual Storage Console provides rapid backup and recovery of multi-host configurations running on N series storage systems.

You can use this capability to do the following tasks:

- Perform on-demand backups of individual virtual machines, datastores, or a datacenter
- Schedule automated backups of individual virtual machines, datastores, or a datacenter

- Support virtual machines and datastores that are located on either NFS directories or VMFS file systems
- Mount a backup to verify its content prior to restoration
- Restore datastores or virtual machines to the original location
- Restore virtual machine disks (VMDKs) to the original or an alternate location
- Restore one or more files to a guest VMDK without having to restore the entire virtual machine or VMDK using single file restore feature

To configure your storage systems, click the N series icon in the vCenter Server and click **Setup** under Backup and Recovery in the navigation pane. The Setup panel displays. Click **Add** on the left side and register your N series system as shown in Figure 14-16.

> **Important:** You must register your N series system three times; first, for the VSC; second, for backup and recovery; and third, for Provisioning and Cloning.

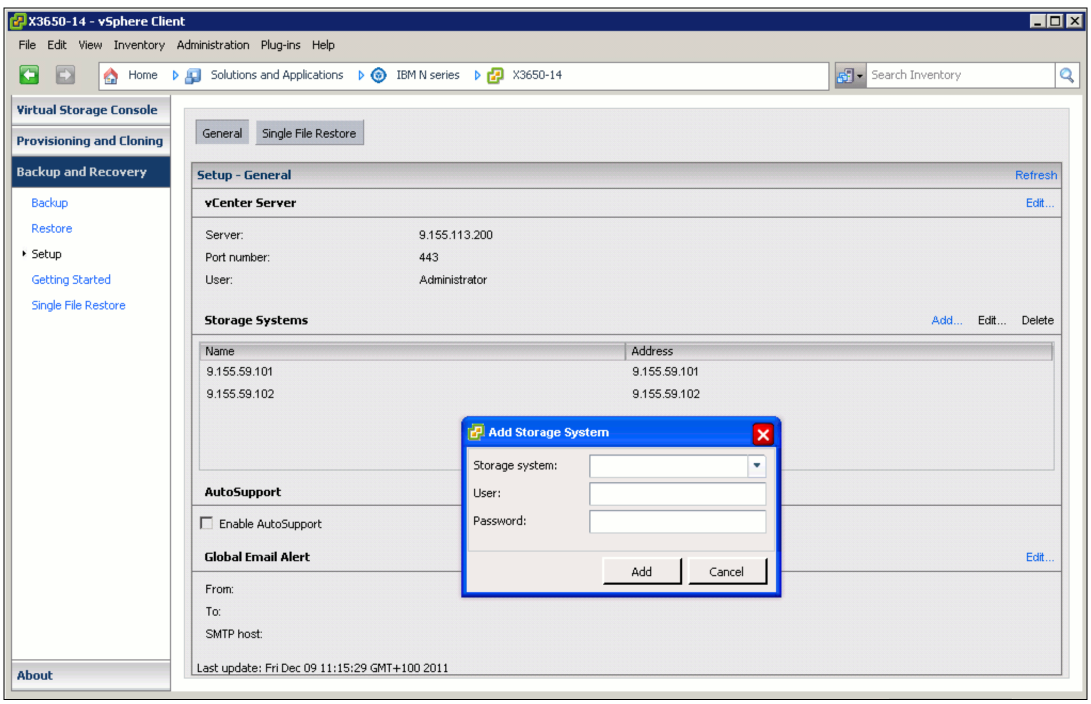



*Figure 14-16 N series registration for backup and restore*

## 14.7.1 Data layout

Layout is indicated by N series best practices for vSphere environments. Move any transient and temporary data, such as the guest operating system swap file, temp files, and page files, to a separate virtual disk on another datastore. The reason is that snapshots of this data type can consume a large amount of storage in a short time because of the high rate of change.

When a backup is created for a virtual machine with VSC, VSC is aware of all VMDKs associated with the virtual machine. VSC initiates a Snapshot copy on all datastores upon which the VMDKs reside. For example, a virtual machine running Windows as the guest operating system has its C drive on datastore ds1, data on datastore ds2, and transient data on datastore td1. In this case, VSC creates a Snapshot copy against all three datastores at underlying volume level. It defeats the purpose of separating temporary and transient data.

### Considerations for transient and temporary data

To exclude the datastore that contains the transient and temporary data from the VSC backup, configure the VMDKs residing in the datastore as "Independent Persistent" disks within the VMware Virtual Center (vCenter). After the transient and temporary data VMDKs are configured, they are excluded from both the VMware Virtual Center snapshot and the N series Snapshot copy initiated by VSC.

You must also create a datastore dedicated to transient and temporary data for all virtual machines with no other data types or virtual disks residing on it. This datastore avoids having a Snapshot copy taken against the underlying volume as part of the backup of another virtual machine. Do not deduplicate the data on this datastore.

SnapManager 2.0 for Virtual Infrastructure can include independent disks and exclude datastores from backup.

### Including independent disks and excluding datastores

You can avoid having a Snapshot copy performed on the underlying volume as part of the backup of another virtual machine. In this case, preferably, create a datastore that is dedicated to transient and temporary data for all virtual machines. Exclude datastores that contain transient and temporary data from the backup. By excluding those datastores, snapshot space is not wasted on transient data with a high rate of change. In VSC 2.0, when selected entities in the backup span multiple datastores, one or more of the spanning datastores might be excluded from the backup.

After configuration, the transient and temporary data .vmdk are excluded from both the VMware vCenter Snapshot and the N series Snapshot copy initiated by VSC. In VSC 1.0, datastores with only independent disks were excluded from the backup. In VSC 2.0, an option is available to include them in the backup. Datastores with a mix of independent disks and normal disks or configuration files for a VM are included in the backup irrespective of this option.

If you have a normal disk and an independent disk for backup on the same datastore, it is always included for backup irrespective of the "include datastore with independent disk" option. Designate a separate datastore exclusively for swap data.

> **Restore from backup:** If you exclude non-independent disks from the backup of a VM, that VM cannot be completely restored. You can perform only virtual disk restore and single file restore from such a backup.

## 14.7.2 Backup and recovery requirements

Your datastore and virtual machines must meet the following requirements before you can use the Backup and Recovery capability:

- In NFS environments, a FlexClone license is required to mount a datastore, restore guest files, and restore a VMDK to an alternate location.
- Snapshot protection is enabled in the volumes where those datastore and virtual machine images reside.
- SnapRestore is licensed for the storage systems where those datastore and virtual machine images reside.

## 14.7.3 Single wizard for creating backup jobs

With the wizard, you can create manual and scheduled backup jobs. In the right pane, you click **Backup**, name your new backup job, and select the per-backup job options:

- Initiate SnapMirror update.
- Perform VMware consistency snapshot.
- Include datastores with independent disks.

### Virtual Machine backup

To back up individual VMs, follow these steps:

1. Right-click the **VM Backup** and drill down until you reach the selection to run or schedule a backup, as shown in Figure 14-17.

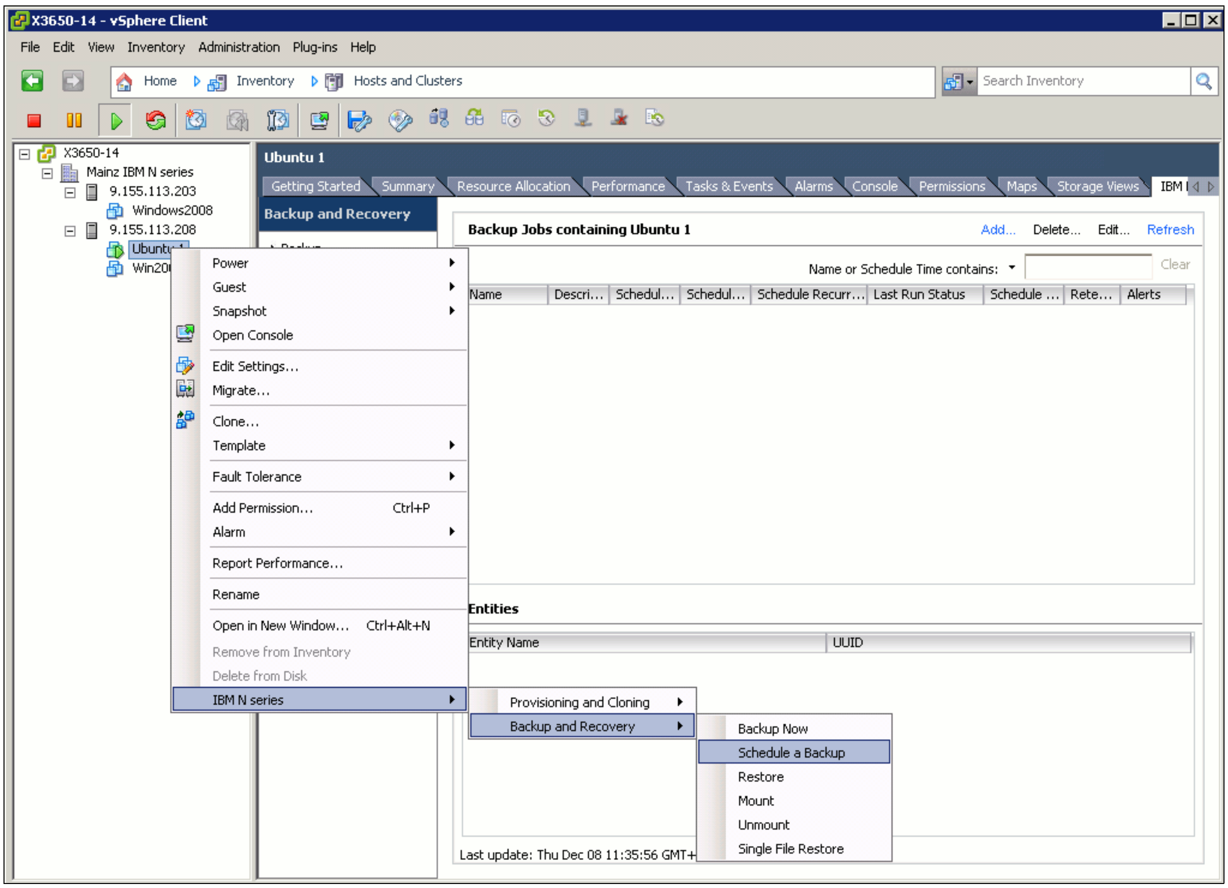



*Figure 14-17 Adding a backup*

2. Go to the Welcome panel, and then click **Next**.
3. Set a Name and Description, specify possible SnapMirror update, or include independent disks (see Figure 14-18), then click **Next**.

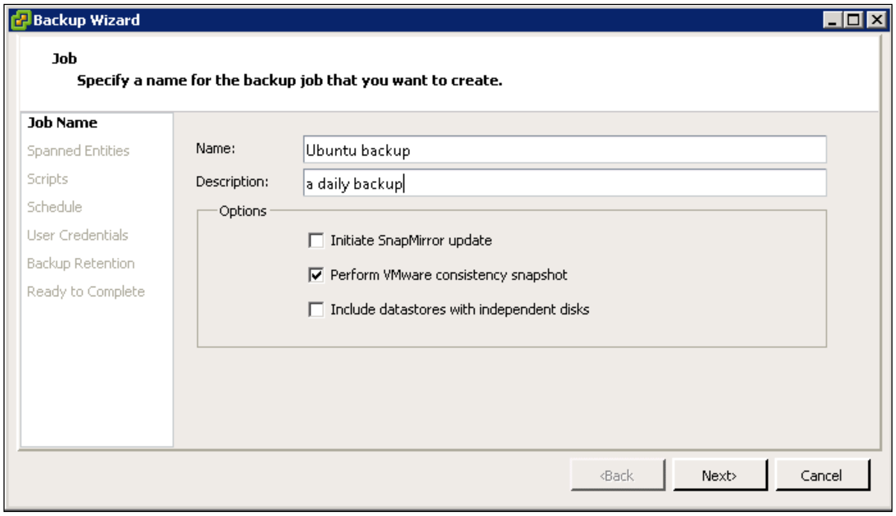



*Figure 14-18 Backup options*

4. Following, you can select scripts to be included in the backup job (see Figure 14-19).

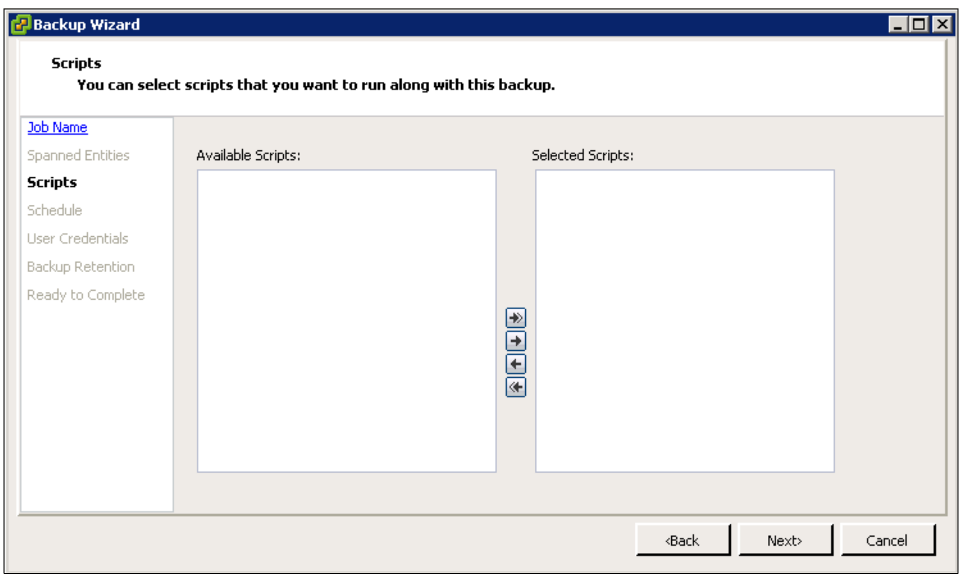



*Figure 14-19 Backup scripts*

5. Now you can specify the schedule for the backup job as in Figure 14-20, and click **Next**.

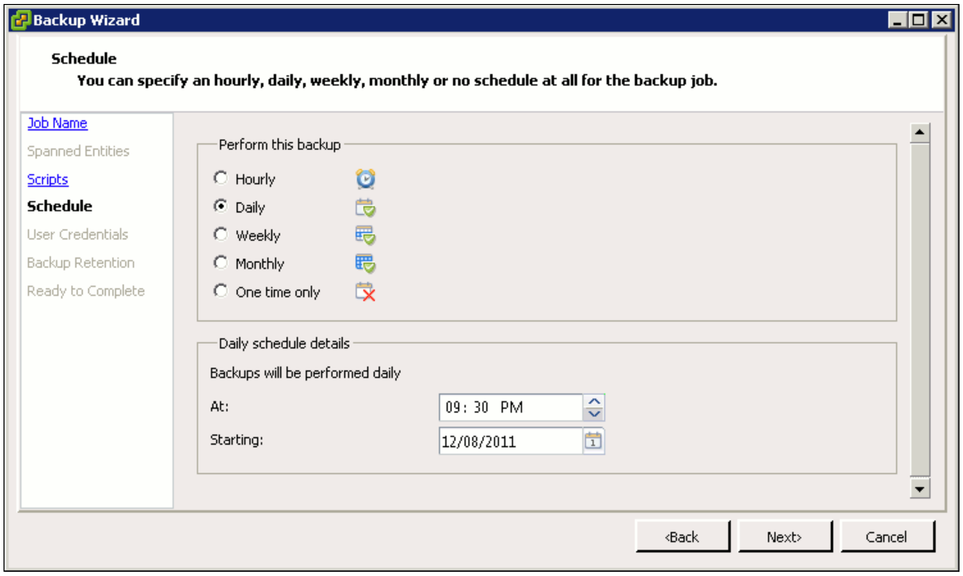



*Figure 14-20 Backup schedule*

6. Confirm your credentials on the next panel as in Figure 14-21, and click **Next**.

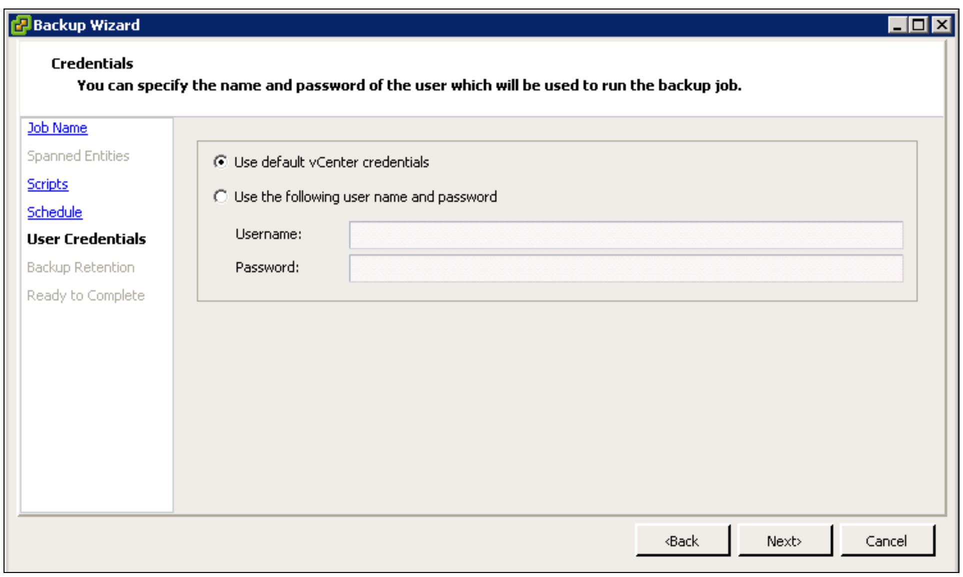



*Figure 14-21 Backup job credentials*

7. Revise the information entered and click **Finish** on the Schedule a Backup Wizard and click **Next**.

8. Select to run your new backup job immediately if you want, as shown in Figure 14-22.

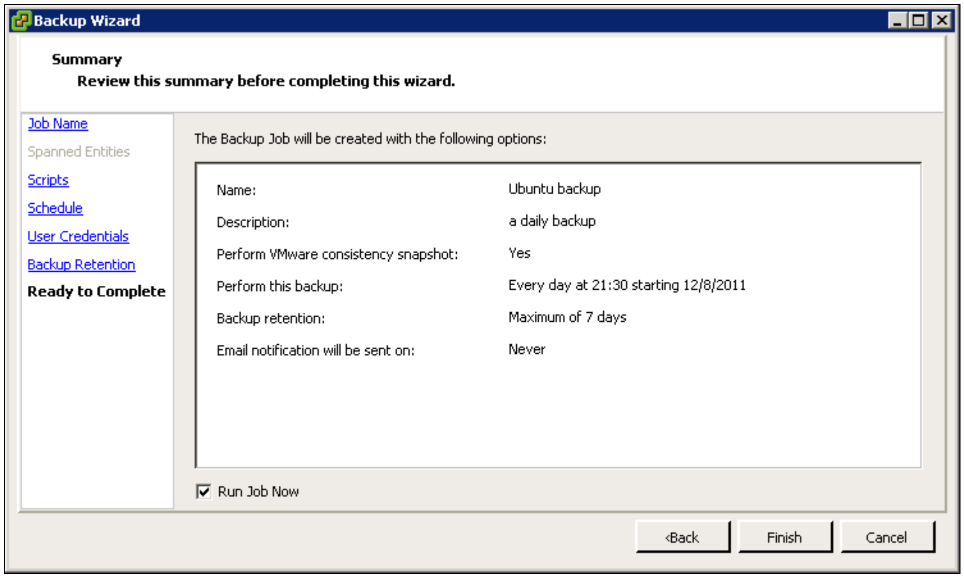



*Figure 14-22 Revise scheduled backup job*

## Datacenter backup

Alternatively, you can also select to back up the whole datacenter as shown in Figure 14-23. Some options are then added to the previously described process.

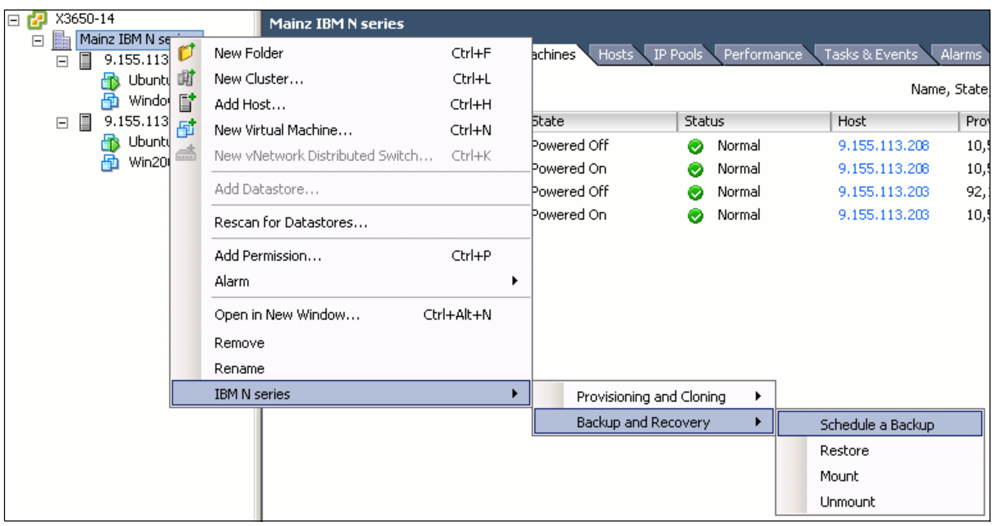



*Figure 14-23 Datacenter backup*

The backup wizard adds the option to select the whole datacenter of backup individual datastores as displayed in Figure 14-24.

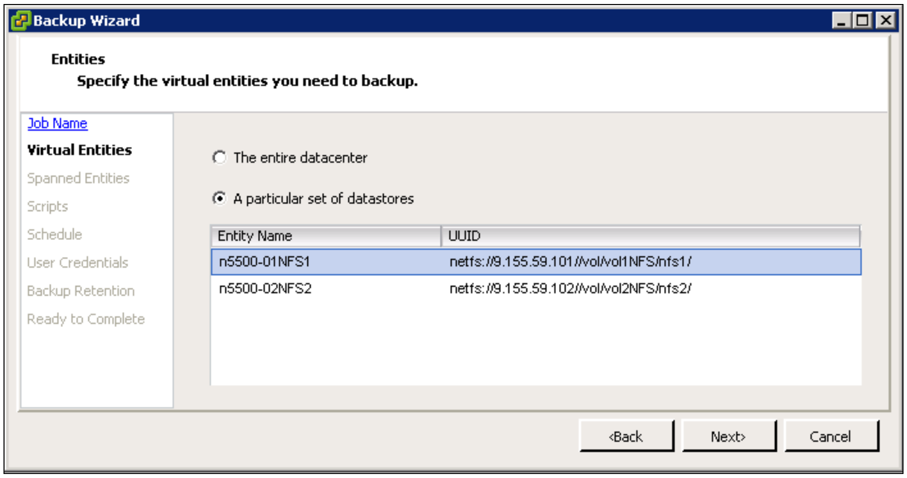



*Figure 14-24 Datacenter backup options*

## Datastore backup

Alternatively, you can also select to back up an individual datastore as shown in Figure 14-24. Some options are then added to the previously described process.

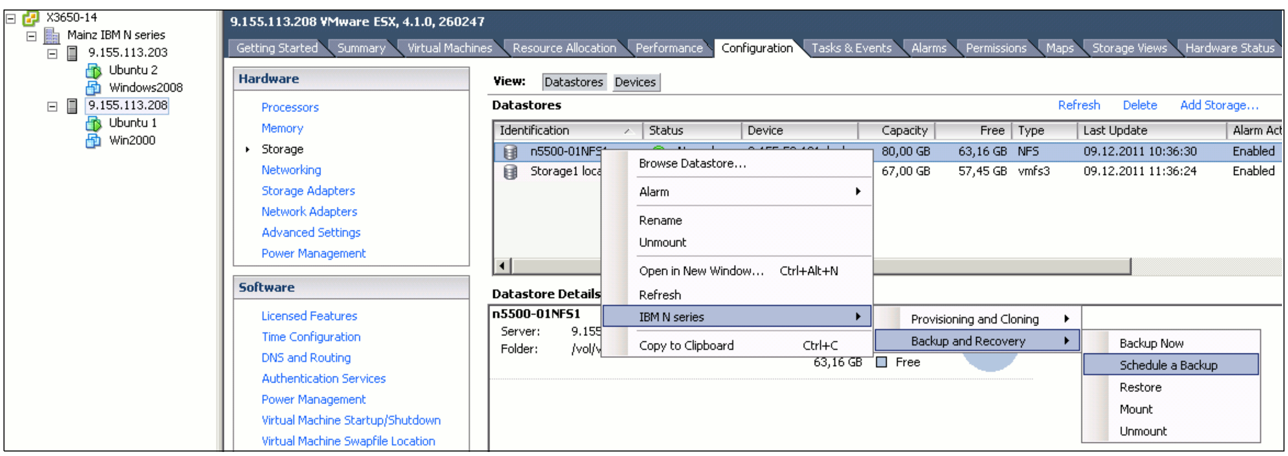



*Figure 14-25 Datastore backup*

The backup wizard adds the option to select the whole datastore of backup individual datastores as displayed in Figure 14-26.

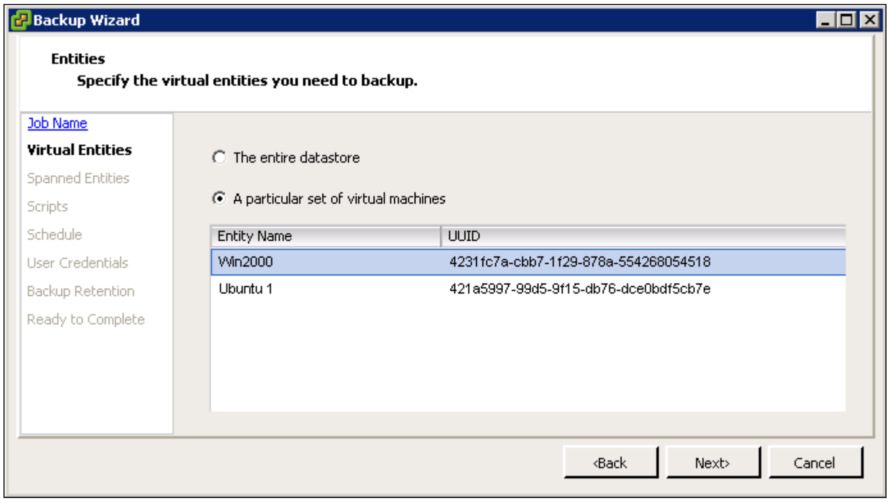



*Figure 14-26 Datastore backup options*

## 14.7.4 Granular restore options

The following granular restore options are available:

- Restore datastores or virtual machines to the original location.
- Restore virtual machine disks (VMDKs) to the original or an alternate location.
- Restore one or more files to a guest VMDK without having to restore the entire virtual machine or VMDK using single file restore feature.

You can access these options by the tabs as shown in Figure 14-27. Right-click the object that you want to restore.

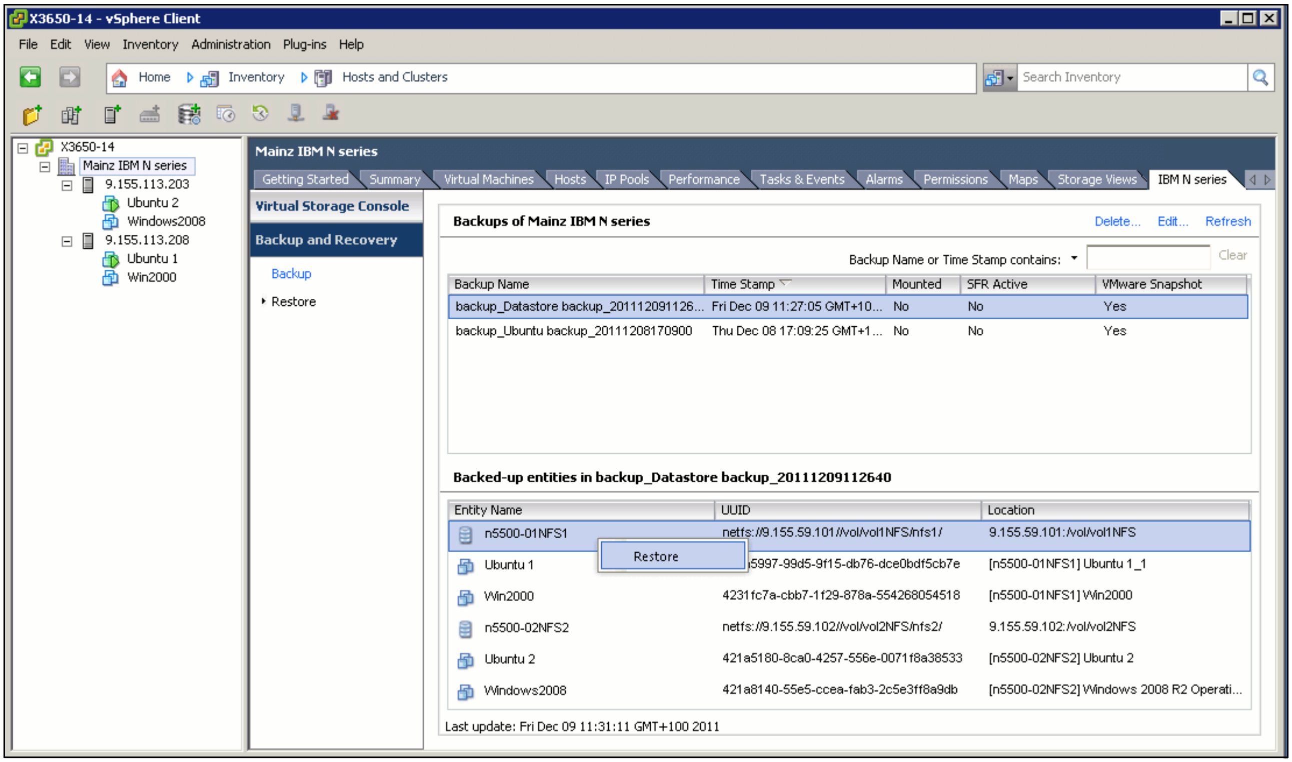



*Figure 14-27 Restore options*

You can also select whether you want to restore the entire virtual machine or individual virtual disks, as in Figure 14-28. Furthermore, you can select the original or a new location.

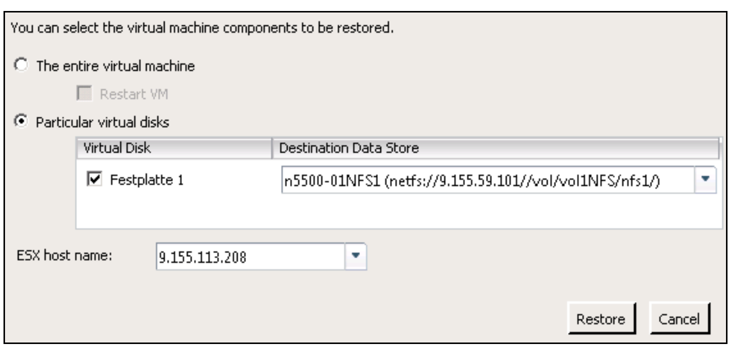



*Figure 14-28 VSC enhanced restore options*

## 14.7.5 Other features

In addition, VSC offers these features:

- Consistent backup naming
- Serialization of VMware vSphere snapshots
- AutoSupport (ASUP) logging
- vFiler unit support for multiple IP addresses
- Advanced Find option to find specific backups

## 14.8 Provisioning and Cloning

This section provide information and examples of the Provisioning and Cloning functions integrated in VSC.

### 14.8.1 Features and functions

The provisioning features require al least Data ONTAP 7.3.3 to accomplish the following tasks:

- Creation, resizing, and deletion of VMFS/NFS datastores
- Ability to provision, clone, and resize volumes on secure vFiler units
- Adding storage system using a domain account
- Automation of pathing for both LUNs and NFS datastores
- Running deduplication operations
- Monitoring storage savings and performance
- Protection against failover of NFS mounts to non-redundant VMkernel ports by limiting multiple TCP sessions to iSCSI only

The cloning features allow you to perform the following tasks:

- Creation of multiple virtual machine clones in new or existing datastores (using FlexClone technology)
- Application of guest customization specifications and powering up of new virtual machines
- Redeployment of virtual machines from a baseline image
- Importing virtual machines into virtual desktop infrastructure connection brokers and management tools
- Clone misalignment alert and prevention:
  - VM misalignment detection and user notification
  - Support for VMFS- and NFS-based VMs
- Ability to import virtual machine settings from a file:
  - Non-contiguous virtual machine names
  - Guest customization specifications
  - Computer name as virtual machine name
  - Power-on settings
- Support for these products:
  - VMware View 4.0, 4.5, 4.6 & 5.0
  - Citrix XenDesktop 4.0 and 5.0

Further features are included:

- Space reclamation management
- Addition of new datastores to new ESX Servers within a cluster
- Service catalog-based provisioning API with enhanced SOAP API to support creation, deletion, and resizing of NFS/VMFS datastores by Storage Services in Provisioning Manager
- Space Reclamation Management

- Mounting of existing datastores when new ESX hosts are added to a cluster or datacenter with support for both NFS and VMFS datastores
- Capability for the user to mount any existing datastore to newly added ESX hosts:
  - VDI One-click Golden Template distribution
  - This feature allows the user to copy a datastore from a source vCenter to one or more target vCenters
- VMware Virtual Desktop Infrastructure (VDI) enhancements:
  - XenDesktop/View import from API
  - VDI One-click Golden Template distribution
  - Saving of View credentials
  - Soap API support for importing newly created clones into Citrix XenDesktop and VMware View
  - Storing of View Server credentials
  - Elimination of the need to add VMware View Server credentials each time by the cloning wizard
  - Creation of multiple View Server pools

### 14.8.2 Provision datastores

The Provisioning and Cloning feature of the VSC 2.0 currently requires reauthentication of storage arrays by specifying the credentials necessary for communication.

> **Important:** You must register your N series system three times; first, for the VSC, second, for backup and recovery; and third, for Provisioning and Cloning.

To do this using the vSphere client, complete the following steps (see Figure 14-29):

1. Connect to vCenter.
2. Select the N series icon on the Home panel.
3. Select the Provisioning and Cloning tab on the left side.
4. Click the **Add** button to begin the Controller Configuration wizard.

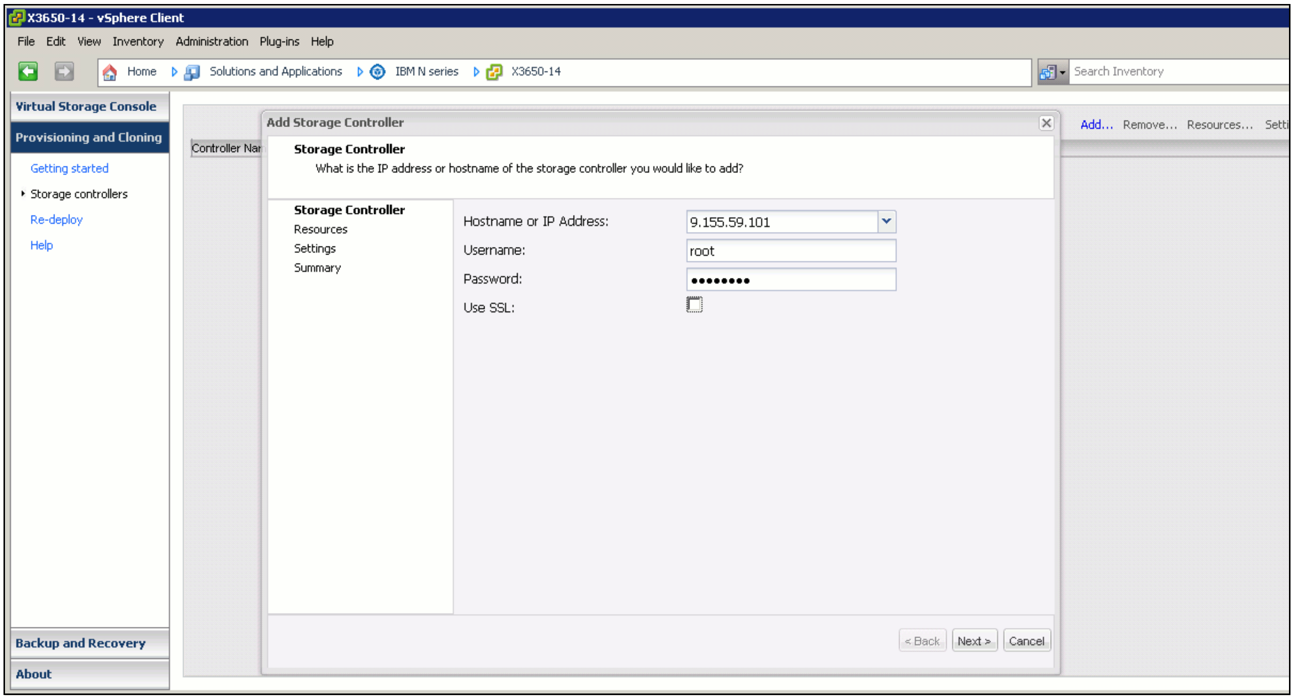



*Figure 14-29 Provisioning and Cloning add controller*

You can create new datastores at the datacenter, cluster, or host level. The new datastore displays on every host in the datacenter or the cluster.

This process launches the N series Datastore Provisioning wizard, which allows you to select the following features:

- Storage controller
- Type of datastore (VMFS or NFS)
- Datastore details, including storage protocol and block size (if deploying a VMFS datastore)
- Specifying whether the LUN should be thin-provisioned

The provisioning process connects the datastore to all nodes within the selected group. For iSCSI, FC, and FCoE datastores, the VSC handles storage access control as follows:

- Creating initiator groups
- Enabling ALUA
- Applying LUN masking
- Applying path selection policies
- Formatting the LUN with VMFS

For NFS datastores, the VSC handles storage access control by managing access rights in the exports file, and it balances the load across all available interfaces.

**Tip:** Remember, if you plan to enable data deduplication, then thin-provisioned LUNs are required to return storage to the free pool on the storage controller.

Follow these steps:

1. In the vSphere Client Inventory, right-click a datacenter, cluster, or host and select **N series** → **Provisioning and Cloning** → **Provision datastore** (see Figure 14-30).

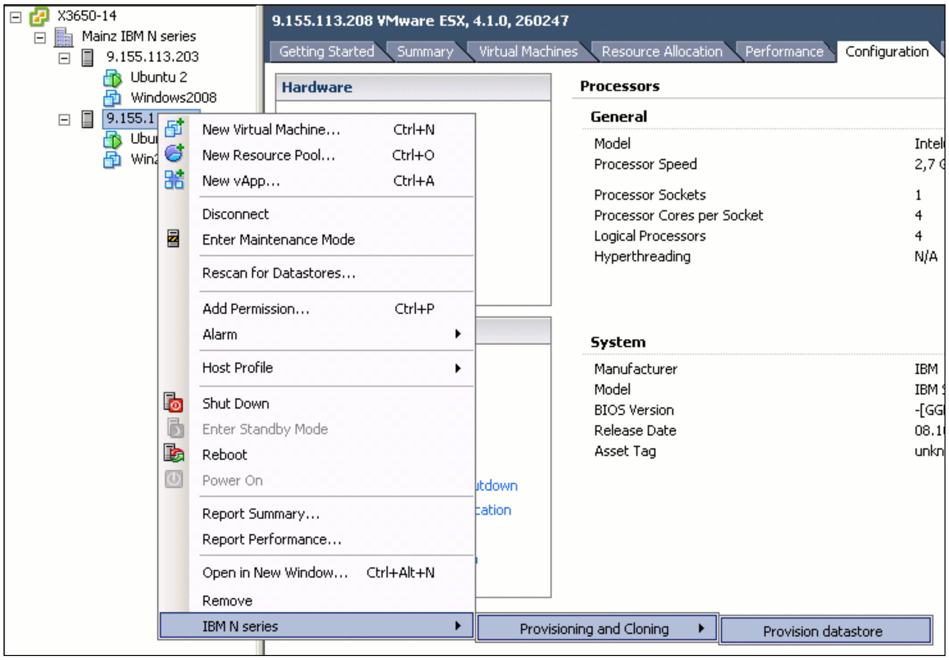



*Figure 14-30 Provision a datastore*

2. Next specify the N series system to use (see Figure 14-31).


*Figure 14-31 Select storage controller for provisioning*

3. Following, select the protocol to use. Here we only have NFS available, as shown in Figure 14-32.

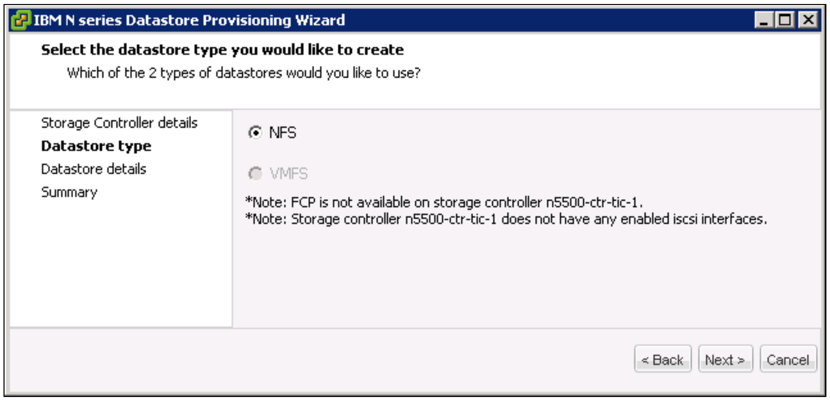



*Figure 14-32 Specify datastore type*

4. Now specify the new datastore details (see Figure 14-33).

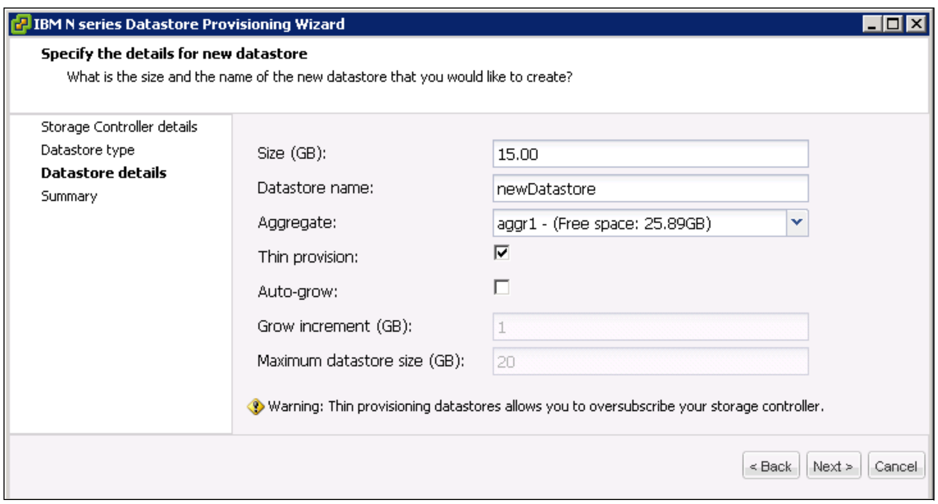



*Figure 14-33 New datastore details*

5. Before applying your selection, verify the information as shown in Figure 14-34.

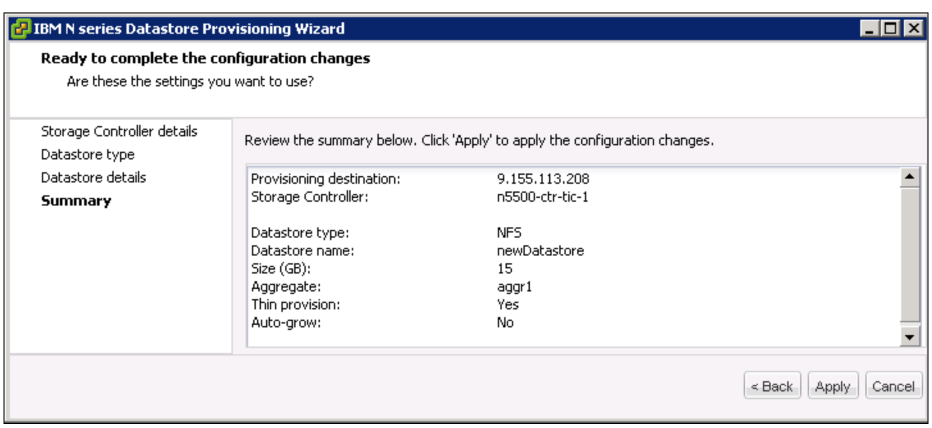



*Figure 14-34 Review new datastore settings*

The new datastore named *newDatastore* was created on the N series. It can now be mounted to the host you want. Figure 14-35 shows FilerView access and the NFS exports.

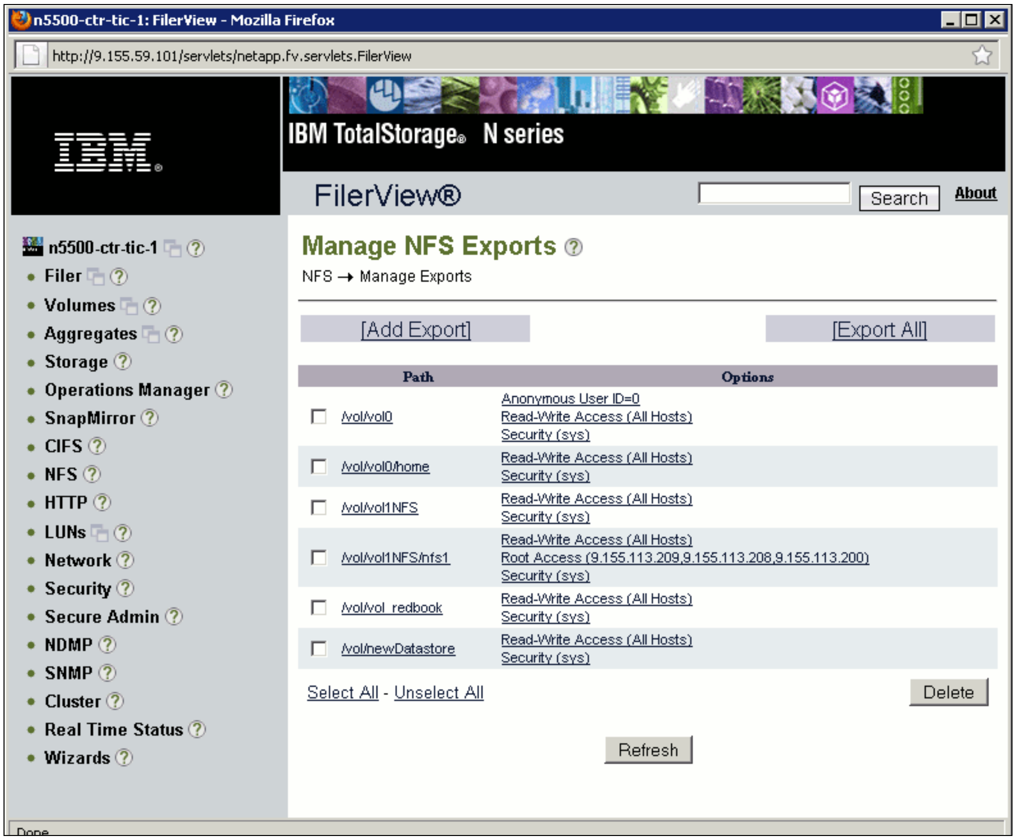


Figure 14-35 Verify NFS exports

## 14.8.3 Managing deduplication

Deduplication eliminates redundant objects on a selected datastore and only references the original object. Figure 14-36 shows how VSC is able to manage deduplication for each individual datastore.

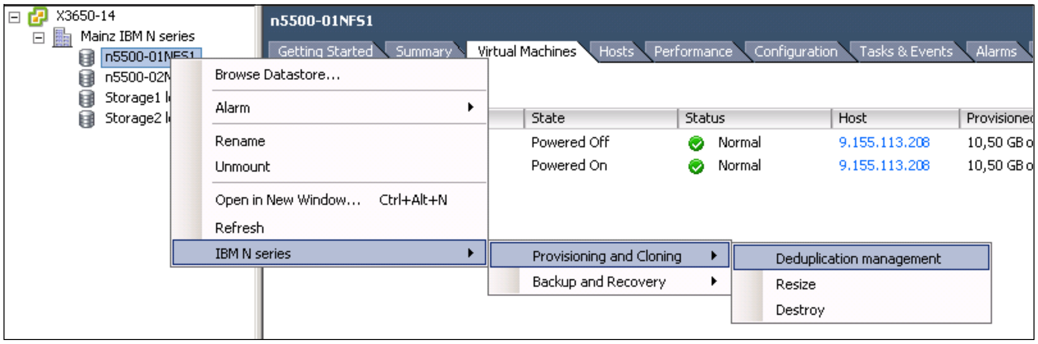



*Figure 14-36 Managing deduplication*

Possible options to use N series advanced deduplication features are displayed in Figure 14-37. Click **OK** to apply your settings.

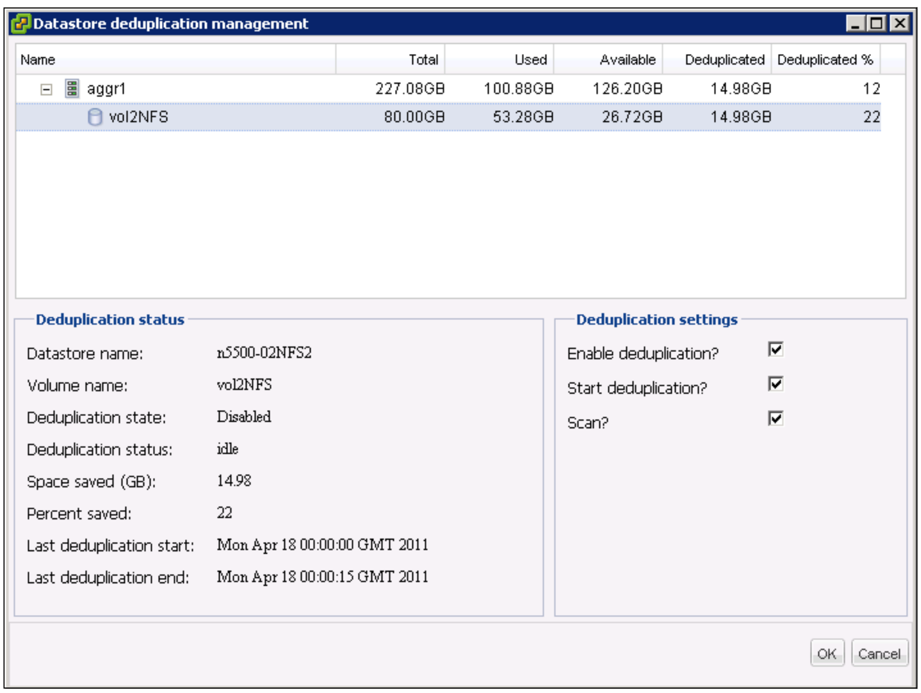



*Figure 14-37 Manage deduplication features*

### 14.8.4 Cloning virtual machines

The Provisioning and Cloning capability can theoretically create thousands of virtual machine clones and hundreds of datastores at one time. In practice, however, multiple executions of fewer requests are preferred. The exact size of these requests depends on the size of the vSphere deployment and the hardware configuration of the vSphere Client managing the ESX hosts.

Follow these steps:

1. In the vSphere Client Inventory, right-click a powered-down virtual machine (Figure 14-38) or template and select **N series** → **Provisioning and Cloning** → **Create rapid clones**.

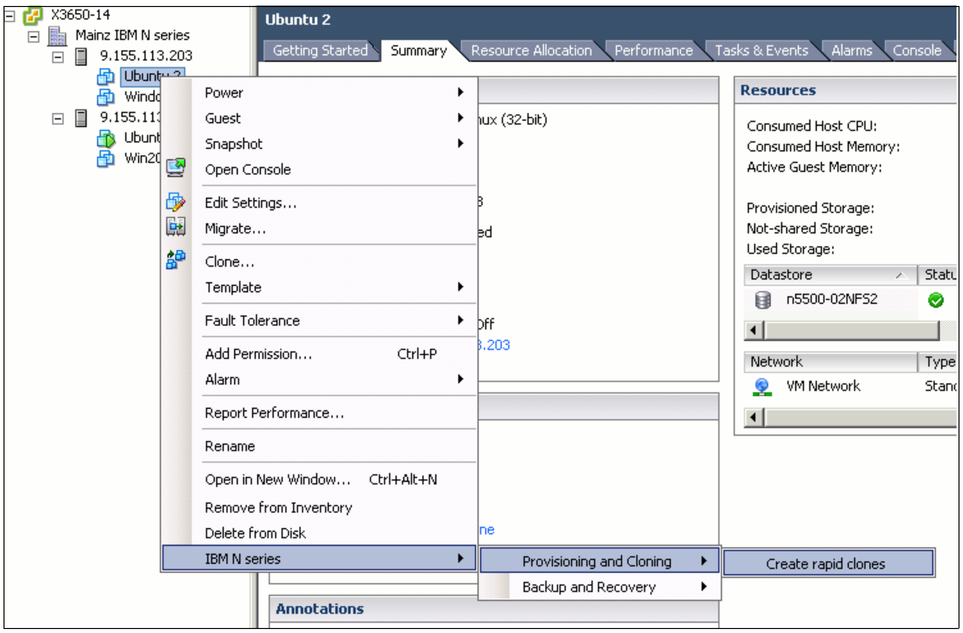



*Figure 14-38 Select VM for cloning*

2. Next select the controller you want to use for cloning (see Figure 14-39).

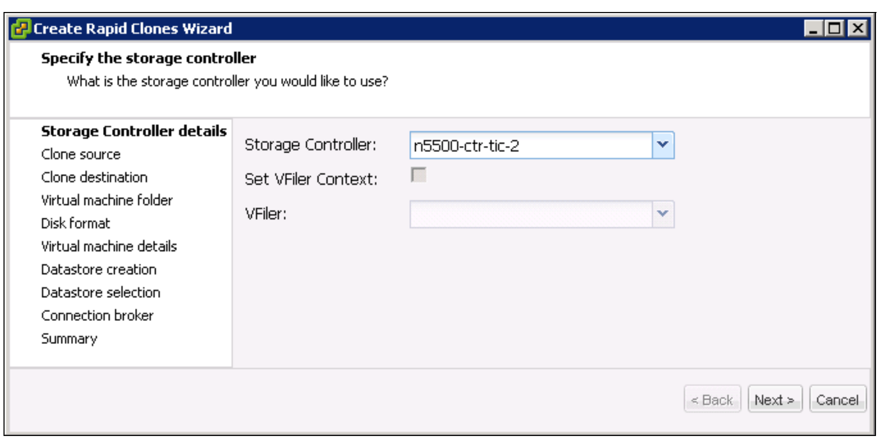



*Figure 14-39 Select controller for cloning*

3. Following, select the destination N series system (see Figure 14-40).

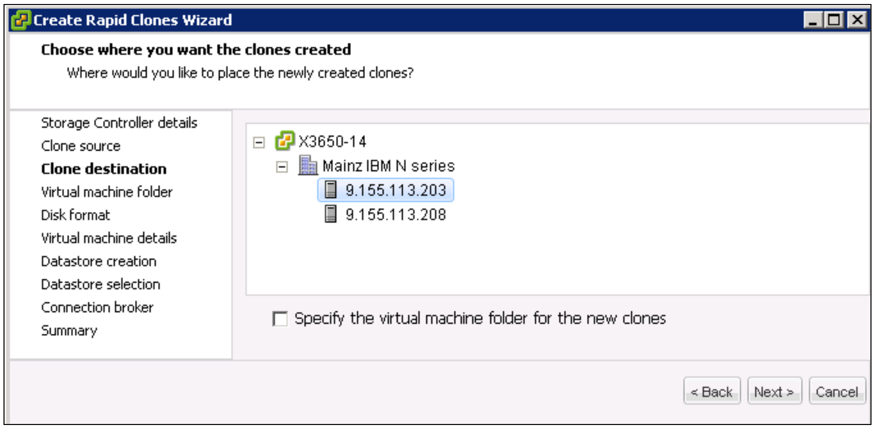



*Figure 14-40 Select clone target*

4. Now specify the VM format for the clone as shown in Figure 14-41.

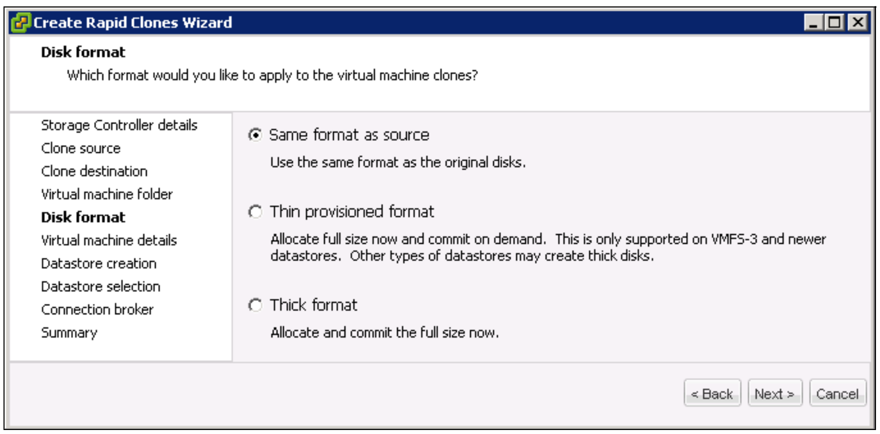



*Figure 14-41 Clone VM format*

5. In the following window, specify details for the new datastores as displayed in Figure 14-42.

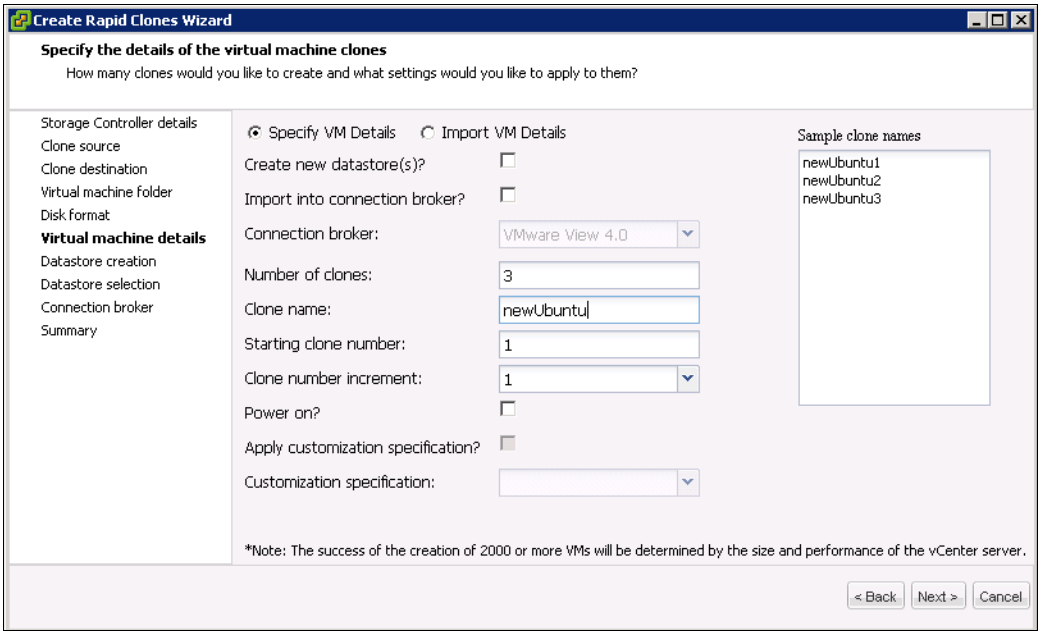



*Figure 14-42 Clone VM details*

6. When a summary is provided (Figure 14-43), click **Apply** to execute your selection.

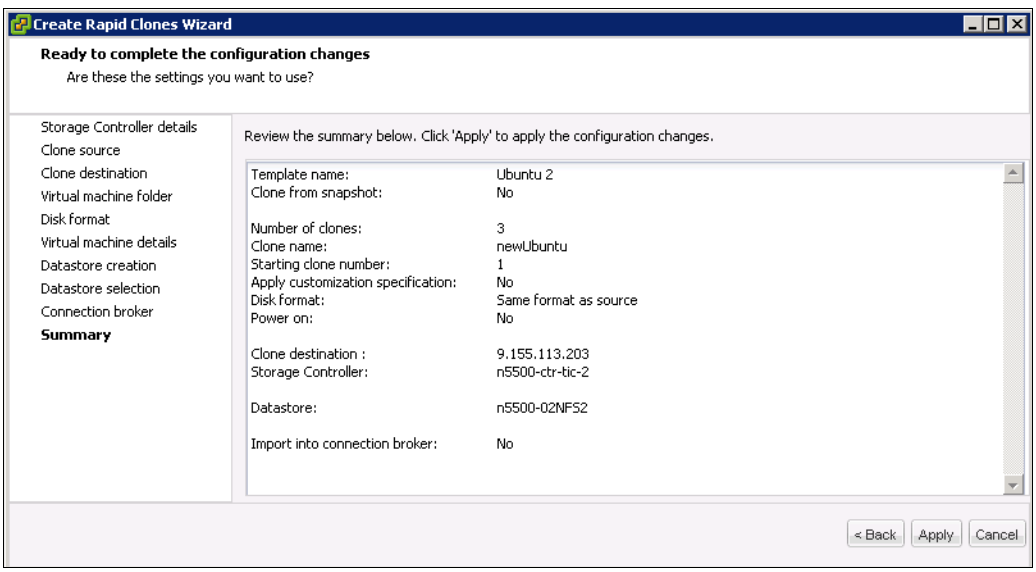



*Figure 14-43 Summary for cloning*

After successful completion of the cloning tasks, the new VMs are configured and ready for further use. Figure 14-44 shows the cloning results.

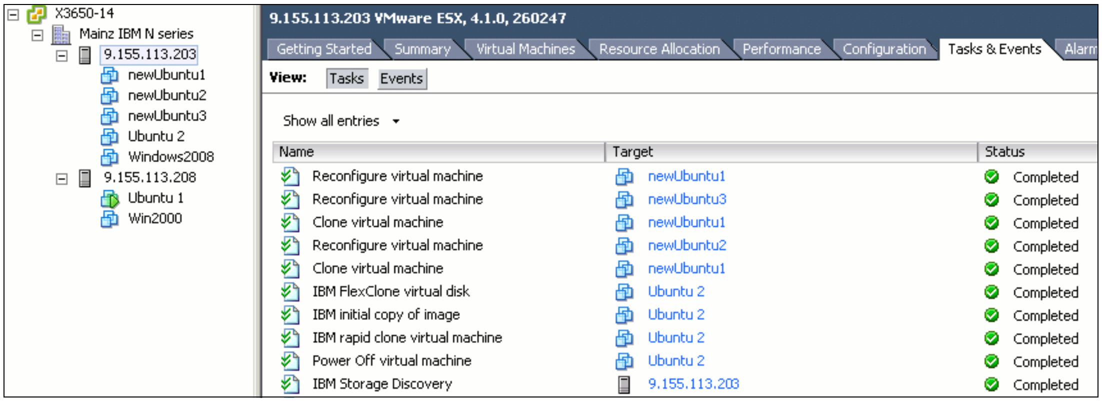


*Figure 14-44 Clone results*

## 14.9 SnapManager for Virtual Infrastructure commands

The SnapManager for Virtual Infrastructure (SMVI) command line interface is still part of the VSC. You can use the Virtual Storage Console command-line interface to perform specific Backup and Recovery capability tasks.

All VSC commands can be performed by using either the GUI or the CLI, with some exceptions. For example, only the creation of scheduled jobs and their associated retention policies and single file restore can be performed through the GUI.

Remember the following general information about the commands:

- SnapManager for Virtual Infrastructure commands are case-sensitive.
- There are no privilege levels; any user with a valid user name and password can run all commands.

You can launch the Virtual Storage Console CLI by using the desktop shortcut or the Windows Start menu. Double-click the VSC CLI desktop icon or navigate to **Start** → **All Programs** → **IBM** → **Virtual Storage Console** →**IBM N series VSC CLI**.

## 14.10 Scripting

VSC provides users the ability to run pre, post, and failure backup phase scripts based on SMVI commands as stated in the previous section. These scripts are any executable process on the operating system in which the VSC is running. When defining the backup to run, the pre, post, and failure backup scripts can be chosen by using either the VSC GUI or CLI. The scripts must be saved in the <SMVI Installation>/server/scripts/ directory. Each chosen script runs as a pre, post, and failure backup script.

From the GUI, you can select multiple scripts by using the backup creation wizard or when editing an existing backup job as shown in Figure 14-19 on page 260. The UI lists all files found in the server/scripts/ directory. VSC runs the scripts before creating the VMware snapshots and after the cleanup of VMware snapshots.

When VSC starts each script, a progress message is logged indicating the start of the script. When the script completes, or is terminated by SAN volume controller because it was running too long, a progress message is logged. It indicates the completion of the script and states if the script was successful or failed. If a script is defined for a backup but is not found in the scripts directory, a message is logged stating that the script cannot be found.

The VSC maintains a global configuration value to indicate the amount of time that a script can execute. After a script runs for this length of time, the script is terminated by the VSC to prevent run-away processing by scripts. If VSC must terminate a script, it is implicitly recognized as a failed script and might force termination of the VSC backup in the pre-backup phase.

With the default settings, VSC waits for up to 30 minutes for each script to complete in each phase. This default setting can be configured by using the following entry in the server/etc/smvi.override file:

```
smvi.script.timeout.seconds=1800
```

VSC backup scripts receive input from the environment variables. This way, the input can be sent in a manner that avoids CLI line length limits. The set of variables varies based on the backup phase.

Sample scripts for VSC can be found in Appendix B, “Sample scripts for VSC” on page 281.

A

# Hot backup Snapshot script

This appendix provides a script for performing effortless hot backups of guests at the datastore level. Guests can be grouped into datastores based on their Snapshot or SnapMirror backup policies, allowing multiple recovery point objectives to be met with little effort. Critical application server guests can have Snapshot copies automatically created based on a different schedule than second-tier applications, or test and development guests. The script even maintains multiple versions of snapshots.

The script shown in Example A-1[1] provides managed and consistent backups of guests in a VMware Virtual Infrastructure 3 environment using N series Snapshot technology. It is provided as an example that can easily be modified to meet the needs of an environment.

Backing up guests with this script completes the following processes:

- Quiesces all the guests on a given datastore
- Takes a crash-consistent N series Snapshot copy
- Applies the redo logs and restores the virtual disk files to a read/write state

*Example A-1 Hot backup Snapshot script*

```
#!/bin/sh
#
# Example code which takes a Snapshot of all guests using the VMware
# vmware-cmd facility. It will maintain and cycle the last 3 Snapshot copies.
#
# This sample code is provided AS IS, with no support or warranties of any
# kind, including but not limited to warranties of merchantability or
# fitness of any kind, expressed or implied.
#
#
# --------------------------------------------------------------------------

PATH=$PATH:/bin:/usr/bin

# Step 1 Enumerate all guests on an individual VMware ESX Server, and put each
# guest in hot backup mode.
```

[1] Original script provided by Vaughn Stewart, NetApp 2007

```
for i in `vmware-cmd -l`
do
  vmware-cmd $i createsnapshot backup Nseries true false
done

# Step 2 Rotate N series Snapshot copies and delete oldest, create new,
# maintaining 3.
ssh <Nseries> snap delete <esx_data_vol> vmsnap.3
ssh <Nseries> snap rename <esx_data_vol> vmsnap.2 vmsnap.3
ssh <Nseries> snap rename <esx_data_vol> vmsnap.1 vmsnap.2
ssh <Nseries> snap create <esx_data_vol> vmsnap.1

# Step 3 Bring all guests out of hot backup mode,
for i in `vmware-cmd -l`
do
  vmware-cmd $i removesnapshots
done
```

B

# Sample scripts for VSC

This appendix provides sample scripts for VSC 2.x that you might find useful for your individual implementation.

## Sample environment variables

Example 14-1 shows environment variables.

*Example 14-1 Environment variables*

```
BACKUP_NAME=My Backup
BACKUP_DATE=20081218
BACKUP_TIME=090332
BACKUP_PHASE=POST_BACKUP
VIRTUAL_MACHINES=3
VIRTUAL_MACHINE.1=VM
1|564d6769-f07d-6e3b-68b1-f3c29ba03a9a|POWERED_ON||true|10.0.4.2
VIRTUAL_MACHINE.2=VM 2|564d6769-f07d-6e3b-68b1-1234567890ab|POWERED_ON|true
VIRTUAL_MACHINE.3=VM 3|564d6769-f07d-6e3b-68b1-ba9876543210|POWERED_OFF|false
STORAGE_SNAPSHOTS=2
STORAGE_SNAPSHOT.1=filer2:/vol/smvi_vol_1:smvi_My_Backup_recent
STORAGE_SNAPSHOT.2=filer2:/vol/smvi_vol_2:smvi_My_Backup_recent
```

## Displaying environment variables during the backup phases

Create a `.bat` file as shown in Example 14-2 to display all environment variables during various backup phases.

*Example 14-2 Displaying variables*

```
echo “==============================”
set >> test.txt
echo “==============================”
```

## SnapVault script for SnapManager for Virtual Infrastructure

The following steps create a sample SnapVault script (Example 14-3):

1. From the command line on an N series storage system, create a new role for the SnapManager for Virtual Infrastructure script:

   `useradmin role add limited-sv-role –a api-snapvault-secondary-initiate-increemental-transfer,login http-admin`

2. Create a user group that uses the previous role:

   `useradmin group add limited-sv-group –r limited-sv-role`

3. Create the actual user:

   `useradmin user add limited-smvi-user –g limited-sv-group`

4. Set the user password:

   `passwd limited-sv-user password`

   Now you have a user who can call only the SnapVault update API.

5. Install the SDK onto the SnapManager for Virtual Infrastructure server.
6. Build your update script and save it in the C:\Program Files\IBM\SMVI\server\scripts directory.

*Example 14-3 SnapVault sample script*

```
if %BACKUP_PHASE% == PRE_BACKUP goto doSNAP
if %BACKUP_PHASE% == POST_BACKUP goto doSV
goto ende
:doSV
chdir "c:\Program Files\IBM\ontapi"
apitest.exe torfiler3 limited-sv-user smv1rocks
snapvault-secondary-initiate-incremental-transfer
primary-snapshot smvi_weeklyBlock1_recent secondary-path
/vol/vmblock1vault/vmblock1
goto ende
:doSNAP
chdir "c:\Program Files\IBM\ontapi"
apitest.exe torfiler3 limited-sv-user smv1rocks
snapvault-secondary-initiate-snapshot-create
schedule-name smvi_weeklyvault volume-name vmblock1vault
goto ende
:ende
EXIT /b 0
```

# Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

## IBM Redbooks publications

The following IBM Redbooks publications provide additional information about the topic in this document. Some publications referenced in this list might be available in softcopy only:


- *IBM System Storage N series Software Guide*, SG24-7129
- *IBM System Storage N series Hardware Guide*, SG24-7840
- *IBM System Storage N series MetroCluster,* REDP-4259
- *IBM N Series Storage Systems in a Microsoft Windows Environment*, REDP-4083
- *IBM System Storage N series A-SIS Deduplication Deployment and Implementation Guide*, REDP-4320
- *IBM System Storage N series with FlexShare*, REDP-4291
- *Managing Unified Storage with IBM System Storage N series Operation Manager*, SG24-7734
- *Using an IBM System Storage N series with VMware to Facilitate Storage and Server Consolidation*, REDP-4211
- *Using the IBM System Storage N series with IBM Tivoli Storage Manager*, SG24-7243


You can search for, view, download or order these documents and other Redbooks publications, Redpaper publications, Web Docs, draft, and additional materials, at the following website:

**ibm.com**/redbooks

## Other publications

These publications are also relevant as further information sources:


- *IBM System Storage N series Data ONTAP 7.3 Storage Management Guide,* GC52-1277-01
- *IBM System Storage N series Data ONTAP 7.2 Core Commands Quick Reference,* GC26-7977-00
- *IBM System Storage N series Data ONTAP 7.2 Network Management Guide*, GC26-7970
- *IBM System Storage N series Data ONTAP 7.2.4 Gateway Implementation Guide for IBM Storage*, GC26-7959
- *IBM System Storage N series Data ONTAP 7.2.3 Gateway Software Setup, Installation, and Management Guide*, GC26-7962

## Online resources

These websites are also relevant as further information sources:

- Network-attached storage:

  http://www.ibm.com/systems/storage/network/

- IBM support: Documentation:

  http://www.ibm.com/support/entry/portal/Documentation

- IBM Storage – Network Attached Storage: Resources:

  http://www.ibm.com/systems/storage/network/resources.html

- Storage Block Alignment with VMware Virtual Infrastructure and IBM System Storage N series:

  ftp://service.boulder.ibm.com/storage/isv/NS3593-0.pdf

- Introduction to VMware vSphere:

  http://www.vmware.com/pdf/vsphere4/r40/vsp_40_intro_vs.pdf

- ESXi Configuration Guides:

  http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esxi_server_config.pdf
  http://www.vmware.com/pdf/vsphere4/r40/vsp_40_esxi_server_config.pdf

- vSphere Datacenter Administration Guides:

  http://www.vmware.com/pdf/vsphere4/r41/vsp_41_dc_admin_guide.pdf
  http://www.vmware.com/pdf/vsphere4/r40/vsp_40_admin_guide.pdf

- All VMware vSphere 4 documentation is located at:

  http://www.vmware.com/support/pubs/vs_pubs.html.

## Help from IBM

IBM Support and downloads:

**ibm.com**/support

IBM Global Services:

**ibm.com**/services

# Index

## E



## F



## G



## H



## I

## O



## P



## Q



## R



## S

# IBM System Storage N series with VMware vSphere 4.1

(0.5” spine)
0.475”<->0.873”
250 <-> 459 pages

# IBM System Storage N series with VMware vSphere 4.1

**Learn how to integrate VMware vSphere with N series**

**Understand Virtual Storage Console features and functions**

**Optimize N series solutions with VMware vSphere**


This IBM Redbooks publication provides a basic introduction to the IBM System Storage N series, virtualization, and VMware. It explains how to use the N series with VMware vSphere 4 environments and the benefits of doing so. Examples are given on how to install and set up VMware ESXi server with the N series.

This edition includes information about the Virtual Storage Console (VSC), which is another N series software product that works with VMware. VSC provides local backup and recovery capability. You have the option to replicate backups to a remote storage system by using SnapMirror relationships. Backups can be performed on individual virtual machines or on datastores with the option of updating the SnapMirror relationship as part of the backup on a per job basis. Similarly, restores can be performed at a data-store level or individual virtual machine level.

IBM System Storage N series in conjunction with VMware vSphere 4 helps complete the virtualization hierarchy by providing both a server and storage virtualization solution. Although this configuration can further assist with other areas of virtualization, networks, and applications, these areas of virtualization are not covered in detail in this book.





SG24-7636-02 ISBN 0738436461