IBM

IBM System Storage N series with VMware vSphere 5

Learn how to integrate VMware vSphere 5.x with N series

Understand Virtual Storage Console features and functions

Optimize N series solutions with VMware vSphere

Roland Tretau
Salahaldean Alamayri
Christian Prediger Appel
João Marcelo Barros de Almeida
Andre Luis Giglioli
William Luiz de Souza

Redbooks

ibm.com/redbooks

International Technical Support Organization

IBM System Storage N series with VMware vSphere 5

February 2013

SG24-8110-00

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

First Edition (February 2013)

This edition applies to the IBM System Storage N series portfolio and Data ONTAP 8.1.1 7-mode as of November 2012.

© Copyright International Business Machines Corporation 2013. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 2013. All rights reserved.

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 grant 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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

© Copyright IBM Corp. 2013. All rights reserved.

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®
DS8000®
Enterprise Storage Server®
HiperSockets™
IBM®
Real-time Compression™
Real-time Compression Appliance™
Redbooks®
Redpapers™
Redbooks (logo) ®
System Storage®
System x®
Tivoli®
XIV®

The following terms are trademarks of other companies:

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

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

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

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 5.x. It explains how to use the N series with VMware vSphere 5 environments and the benefits of doing so. Examples are given on how to install and set up VMware ESXi server with the N series.

The IBM System Storage N series used as a storage foundation offers unified storage solutions that provide industry-leading technologies in the areas of storage efficiencies, instantaneous virtual machine and datastore cloning for virtual servers and virtual desktops, and virtual data center backup and business continuance solutions.

The information provided can be also be used as a foundation to create dynamic cloud solutions, making full use of underlying storage features and functions. This book provides a blueprint for how clients can create a virtualized infrastructure/storage cloud that will help to address current and future data storage business requirements.

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 5 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.

The team who wrote this book

This book was produced by a team of specialists from around the world working at the International Technical Support Organization, San Jose Center.

Roland Tretau is an Information Systems professional with over 15 years experience in the IT industry. He holds Engineering and Business Masters degrees, and is the author of many storage related IBM Redbooks publications. Roland's areas of expertise range from project management, market enablement, managing business relationships, product management, and consulting, to technical areas including operating systems, storage solutions, and cloud architectures.

Salahaldean Alamayri is an IT Professional holding two Masters degrees (an MBA and an MSEE) with both management and technical backgrounds that span over a decade in the Information Technology industry. He has gained embedded systems experience, storage, and backup and recovery technologies experience, and additional background in database design, performance tuning, recovery, and security. He received multiple awards for his contributions in these fields.

© Copyright IBM Corp. 2013. All rights reserved.

Christian Prediger Appel is a Server Specialist with GTS IBM in Brazil who has been working with networking, storage, and server components since 2000. Christian worked for an Internet Service Provider (ISP) and a server management company before joining IBM in 2005, where he now works in designing, implementing, and managing projects, and is an instructor of server technologies. He is focusing on virtualization and cloud technologies and holds certifications from Microsoft, Citrix, VMware, and IBM, as a Certified IT Specialist.

João Marcelo Barros de Almeida is an IT Specialist at IBM Brazil who has extensive experience in operating systems and server virtualization, designing, installing, administering and supporting several environments. He is a Microsoft Certified Systems Administrator (MCSA) and Microsoft Certified Trainer (MCT), and has worked in the IT industry for 12 years.

Andre Luis Giglioli is a NetApp Certified Professional in Brazil who supports business partners around the world. Andre has focal account and subject matter expertise and has over two years of experience with storage NetApp / N series. He works with projects such as deployment and implementation of storage environments. He attended the Hall of Fame IBM 2012 for customer recognition, which he currently supports.

William Luiz de Souza is a Technical Leader at IBM Brazil SO Delivery with over 10 years experience in the IT industry. He holds Systems Information and Business Masters degrees, and has the IBM IT Specialist Level 2 certification. He is also author of other Redbooks publications and Redpaper™ publications. William is experienced and certified in Microsoft, VMware, and Citrix solutions with IBM System x® platforms.

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

Bertrand Dufrasne
IBM International Technical Support Organization, San Jose Center

Uwe Heinrich Mueller, Uwe Schweikhard
IBM Germany

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 publications in one of the following ways:

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

  ibm.com/redbooks

- Send your comments in an email 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

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.

© Copyright IBM Corp. 2013. All rights reserved.

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.

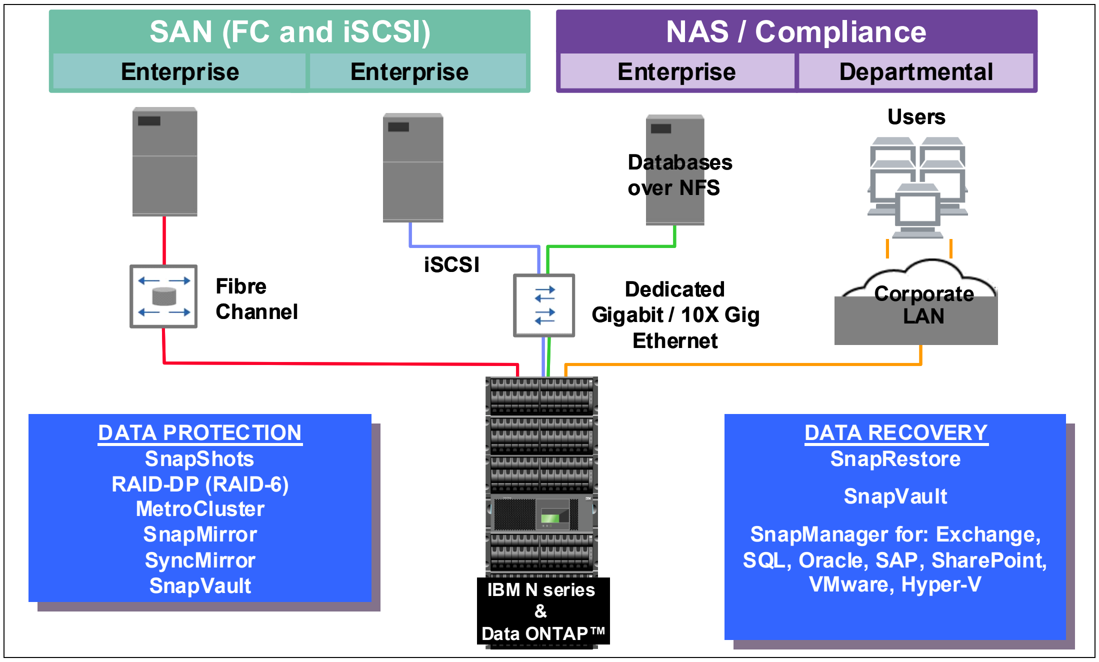


Figure 1-1 N series unified storage

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.

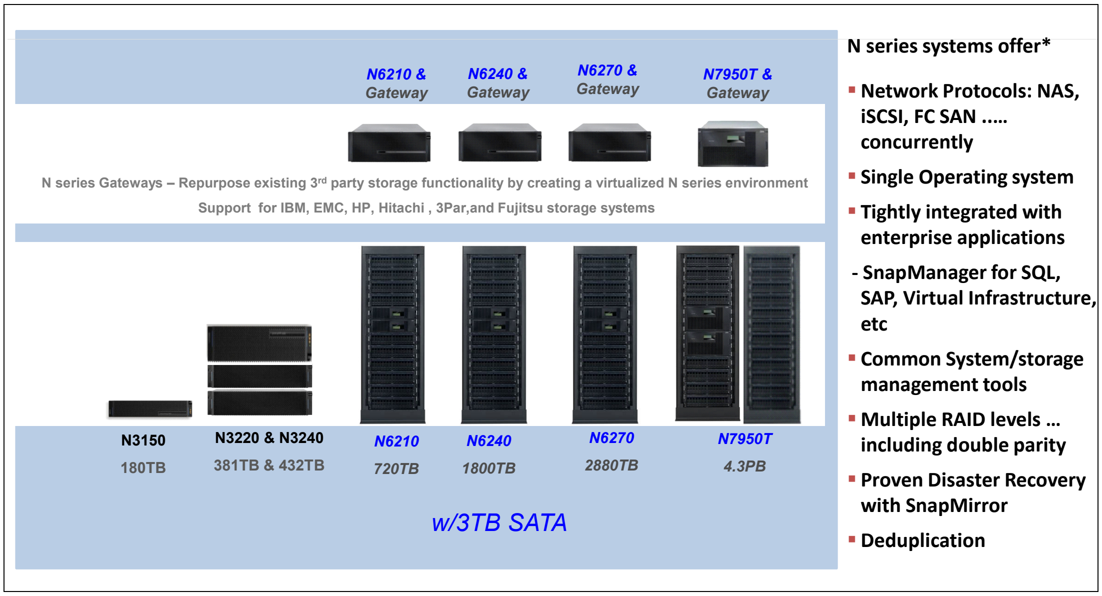
N series units come with pre-configured software and hardware, and with no monitor or keyboard for user access, which is commonly called a *headless system*. A storage administrator accesses the systems and manages the disk resources from a remote console by using a web browser or command line.

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.



N series Gateways – Repurpose existing 3rd party storage functionality by creating a virtualized N series environment

Support for IBM, EMC, HP, Hitachi , 3Par,and Fujitsu storage systems

N series systems offer*

- **Network Protocols: NAS, iSCSI, FC SAN ….. concurrently**
- **Single Operating system**
- **Tightly integrated with enterprise applications**

  - SnapManager for SQL, SAP, Virtual Infrastructure, etc
- **Common System/storage management tools**
- **Multiple RAID levels … including double parity**
- **Proven Disaster Recovery with SnapMirror**
- **Deduplication**

Figure 1-2 N series portfolio

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

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. They 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. It 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.

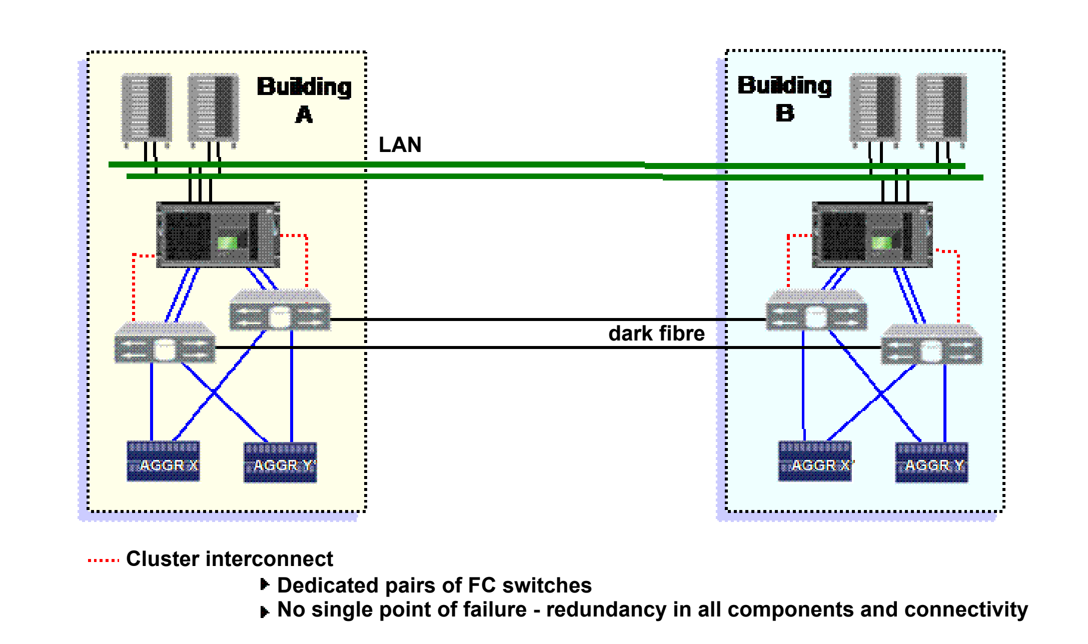

Building A
LAN
Building B
dark fibre
AGGR X
AGGR Y'
AGGR X'
AGGR Y
Cluster interconnect
Dedicated pairs of FC switches
No single point of failure - redundancy in all components and connectivity

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. Included are 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.

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

Table 1-1 Key N series software features overview

Feature	Benefits
Data ONTAP	► Provides full-featured and multiprotocol data management for both block and file serving environments through N series storage operating system. ► Simplifies data management through single architecture and user interface, and reduces costs for SAN and NAS deployment.
Data compression	► Offers transparent inline data compression to store more data in less space, reducing the amount of storage you need to purchase and maintain. ► Reduces the time and bandwidth required to replicate data during volume SnapMirror transfers.
Deduplication	► Performs block-level data deduplication on NearStore data volumes ► Scans and deduplicates volume data automatically, resulting in fast, efficient space savings with minimal impact on operations.
Disk sanitization	► Obliterates data by overwriting disks with specified byte patterns or random data, ► Prevents recovery of current data by any known recovery methods.
Flash Pool (requires Data ONTAP 8.1.1 or later version)	► Enables automated storage tiering and combines solid-state drive (SSD) and hard disk drive (HDD) technology. ► Helps to achieve optimal performance and efficiency while lowering the cost of the storage infrastructure.
FlexCache	► Creates a flexible caching layer within your storage infrastructure that automatically adapts to changing usage patterns to eliminate bottlenecks. ► Improves application response times for large compute farms, speeds data access for remote users or creates a tiered storage infrastructure that circumvents tedious data management tasks.
FlexClone	► Provides near-instant creation of logical unit number (LUN) and volume clones without requiring additional storage capacity. ► Accelerates test and development, and storage capacity savings.
FlexShare	► Prioritizes storage resource allocation to highest-value workloads on a heavily loaded system. ► Ensures that best performance is provided to designated high-priority applications.
FlexVol	► Creates flexibly sized LUNs and volumes across a large pool of disks and one or more RAID groups. ► Enables applications and users to get more space dynamically and nondisruptively without IT staff intervention. ► Enables more productive use of available storage and helps improve performance.

Feature	Benefits
Gateway	► Supports attachment to IBM Enterprise Storage Server® series, IBM XIV® Storage System, IBM System Storage IBM DS8000®, IBM System Storage DS5000 series and a broad range of IBM, EMC, Hitachi, Fujitsu and HP storage subsystems.
MetroCluster	► Offers an integrated high-availability/disaster-recovery solution for campus and metro-area deployments. ► Ensures high data availability when a site failure occurs. ► Supports Fibre Channel attached storage with SAN Fibre Channel switch; SAS attached storage with Fibre Channel/SAS bridge; or Gateway storage with SAN/Fibre Channel switch.
MultiStore	► Partitions a storage system into multiple virtual storage appliances. ► Enables secure consolidation of multiple domains and file servers.
NearStore (nearline)	► Increases the maximum number of concurrent data streams (per storage controller). ► Enhances backup, data protection and disaster preparedness by increasing the number of concurrent data streams between two N series systems.
OnCommand	► Enables the consolidation and simplification of shared IT storage management by providing common management services, integration, security and role-based access controls delivering greater flexibility and efficiency
RAID-DP	► Offers double parity bit RAID protection (N series RAID 6 implementation). ► Protects against data loss due to double disk failures and media bit errors occurring during drive rebuild processes.
SecureAdmin	► Authenticates both the administrative user and the N series system, creating a secure, direct communication link to the N series system. ► Protects administrative logins, passwords and session commands from cleartext snooping by replacing RSH and Telnet with the strongly encrypted SSH protocol.
Single Mailbox Recovery for Exchange (SMBR)	► Enables the recovery of a single mailbox from a Microsoft Exchange Information Store. ► Extracts a single mailbox or email directly in minutes with SMBR, compared to hours with traditional methods, eliminating the need for staff-intensive, complex, and time-consuming Exchange server and mailbox recovery.
SnapDrive	► Provides host-based data management of N series storage from Microsoft Windows, UNIX, and Linux servers. ► Simplifies host-consistent snapshot copy creation and automates error-free restores.
SnapLock	► Write-protects structured application data files within a volume to provide write-once-read-many (WORM) disk storage. ► Provides storage enabling compliance with government records retention regulations.
SnapManager	► Provides host-based data management of N series storage for databases and business applications. ► Simplifies application-consistent snapshot copies, automates error-free data restores, and enables application-aware disaster recovery.

Feature	Benefits
SnapMirror	► Enables automatic, incremental data replication between synchronous or asynchronous systems. ► Provides flexible, efficient site-to-site mirroring for disaster recovery and data distribution.
SnapRestore	► Restores single files, directories, or entire LUNs and volumes rapidly, from any snapshot backup. ► Enables near-instant recovery of files, databases and complete volumes.
Snapshot	► Makes incremental, data-in-place, point-in-time copies of a LUN or volume with minimal performance impact. ► Enables frequent, nondisruptive, space-efficient and quickly restorable backups.
SnapVault	► Exports snapshot copies to another N series system, providing an incremental block-level backup solution. ► Enables cost-effective, long-term retention of rapidly restorable disk-based backups.
Storage encryption	► Provides support for self-encrypting disk (SED) drives in N series disk shelf storage and integration with license key managers, including IBM Tivoli® License Key Manager.
SyncMirror	► Maintains two online copies of data with RAID-DP protection on each side of the mirror. ► Protects against all types of hardware outages, including triple disk failure.
Gateway	► Reduces data management complexity in heterogeneous storage environments for data protection and retention.

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 1-4).

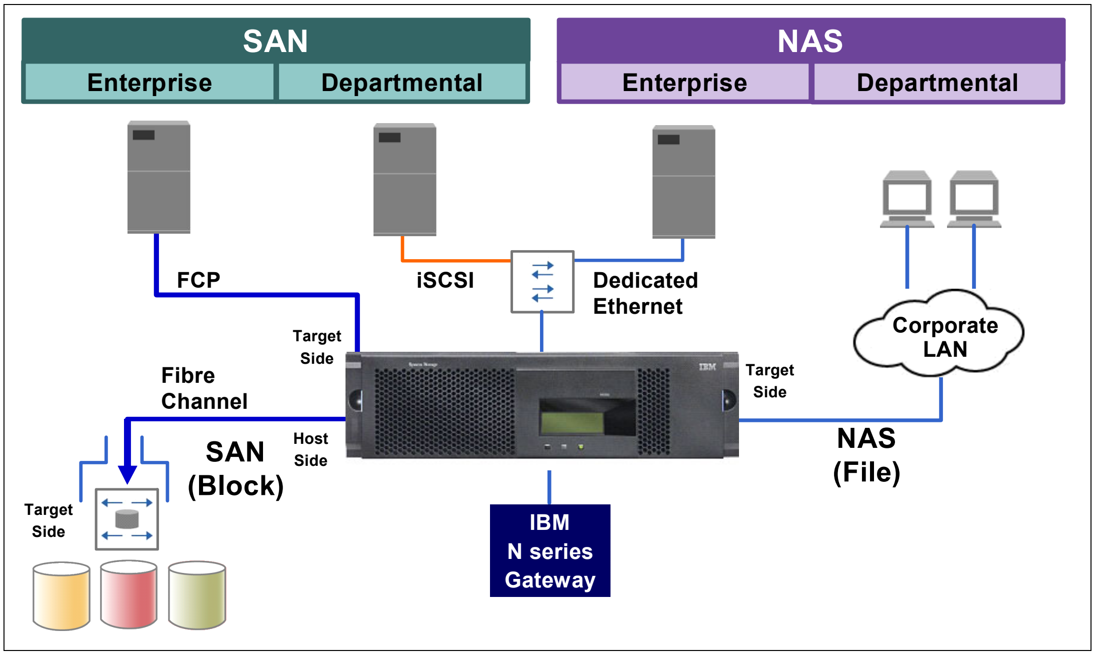


Figure 1-4 Gateway topology

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 1-5).

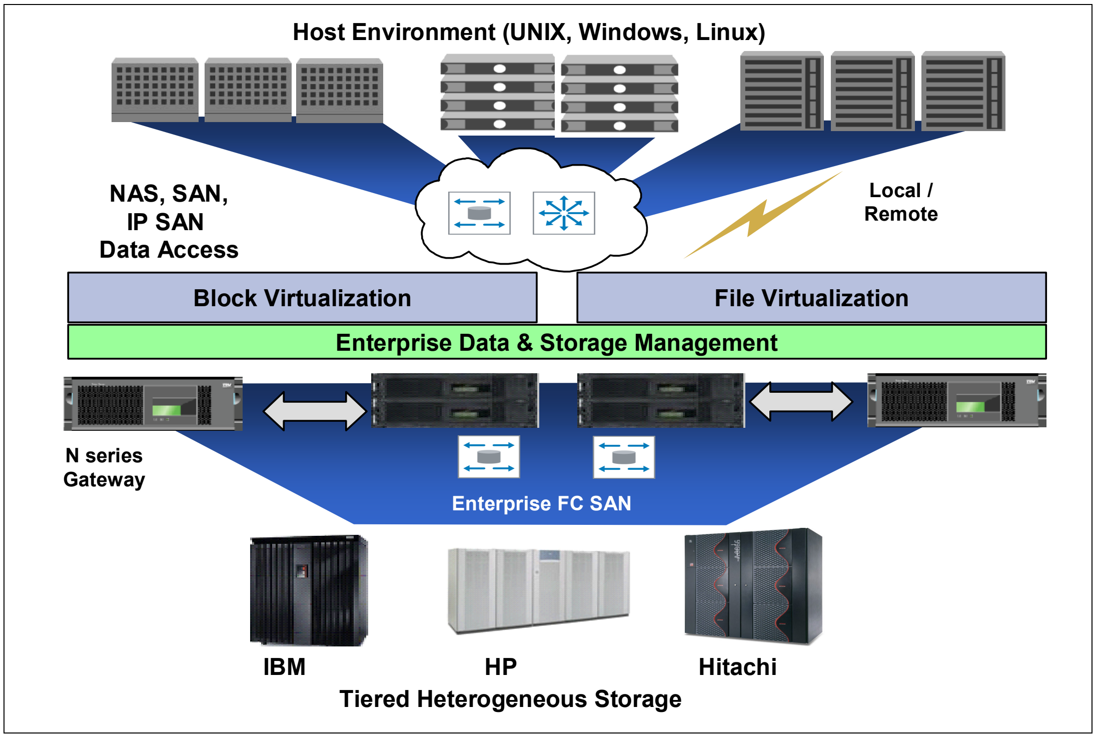


Figure 1-5 Tiered heterogeneous storage

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/SATA Disk Storage Expansion Unit (MTM 2857-003) with 24 slots for SAS disk drives.
- EXN3200: SATA Disk Storage Expansion Unit (MTM 2857-306) with 48 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 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 different SAS loops. EXN3200 shelves can be attached to N62xx and N7950 systems supporting Data ONTAP 8.1.1.

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 1-6.

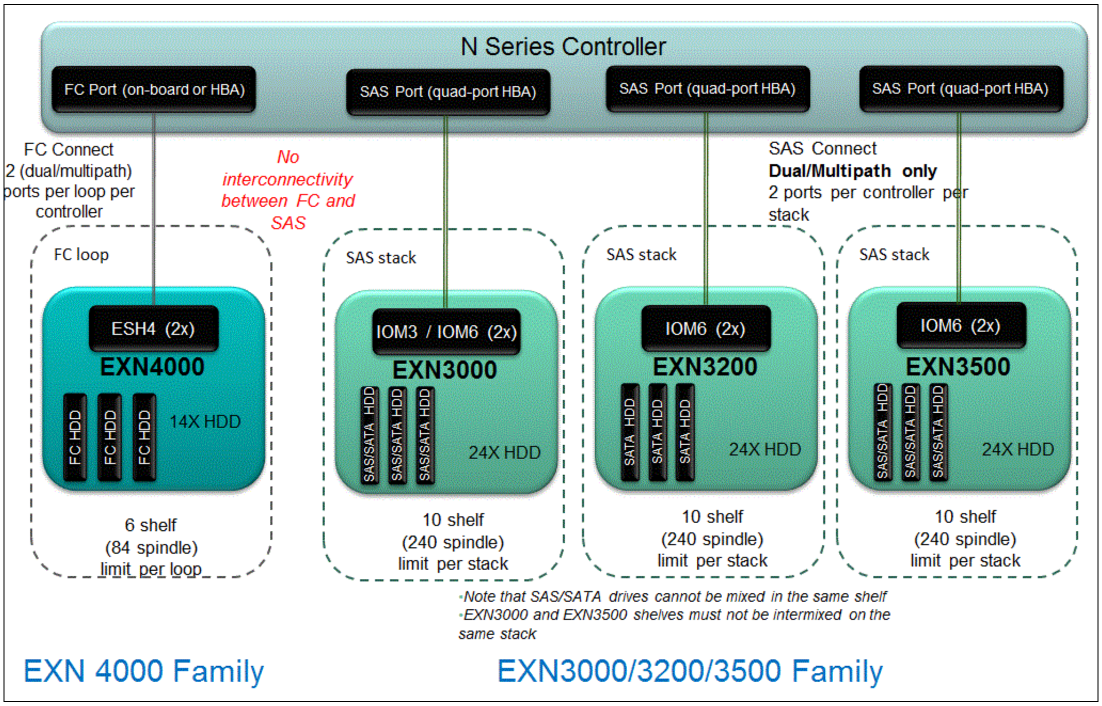

N Series Controller
FC Port (on-board or HBA)
SAS Port (quad-port HBA)
SAS Port (quad-port HBA)
SAS Port (quad-port HBA)
FC Connect
2 (dual/multipath) ports per loop per controller
No interconnectivity between FC and SAS
SAS Connect
Dual/Multipath only
2 ports per controller per stack
FC loop
SAS stack
SAS stack
SAS stack
ESH4 (2x)
EXN4000
FC HDD
FC HDD
FC HDD
14X HDD
IOM3 / IOM6 (2x)
EXN3000
SAS/SATA HDD
SAS/SATA HDD
SAS/SATA HDD
24X HDD
IOM6 (2x)
EXN3200
SATA HDD
SATA HDD
SATA HDD
24X HDD
IOM6 (2x)
EXN3500
SAS/SATA HDD
SAS/SATA HDD
SAS/SATA HDD
24X HDD
6 shelf (84 spindle) limit per loop
10 shelf (240 spindle) limit per stack
10 shelf (240 spindle) limit per stack
10 shelf (240 spindle) limit per stack
•Note that SAS/SATA drives cannot be mixed in the same shelf
•EXN3000 and EXN3500 shelves must not be intermixed on the same stack
EXN 4000 Family
EXN3000/3200/3500 Family

Figure 1-6 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. All of the fragmented application-based storage and unstructured data are consolidated 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.

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 by 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 expendability. It delivers high-end enterprise storage and data management value with midrange affordability.

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

© Copyright IBM Corp. 2013. All rights reserved.

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.

So to summarize, here are the main reasons why you should use virtualization:

- To get more out of your hardware resources
- To reduce IT costs
- To increase hardware and applications availability improving business continuity
- To increase operational flexibility
- To improve desktop manageability and security

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.

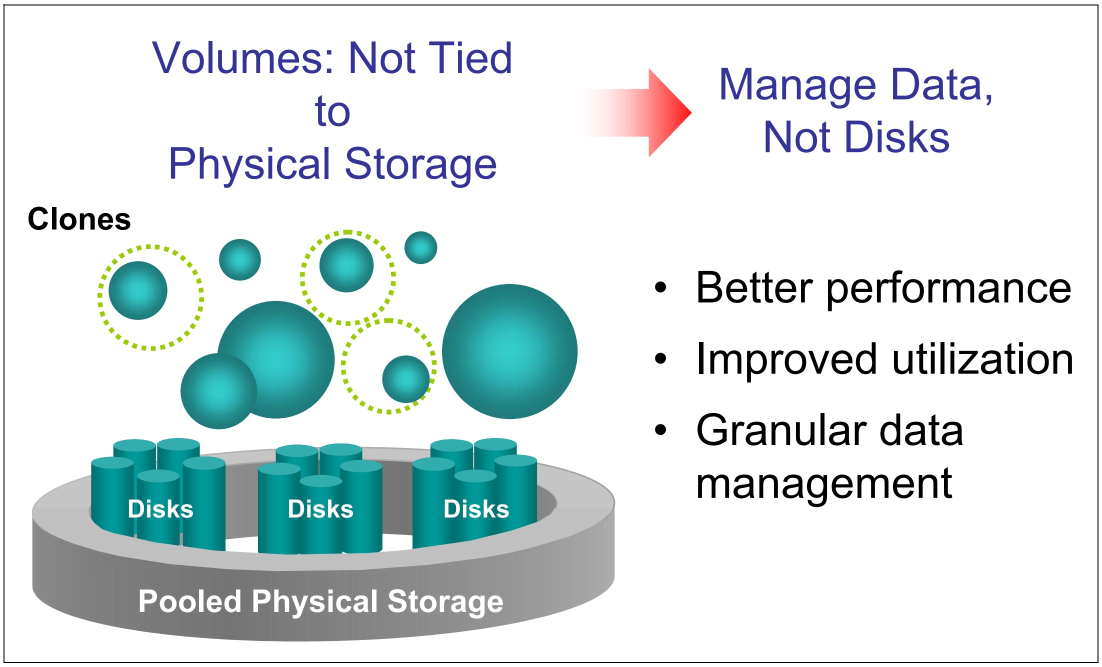


Figure 2-1 Storage virtualization

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.

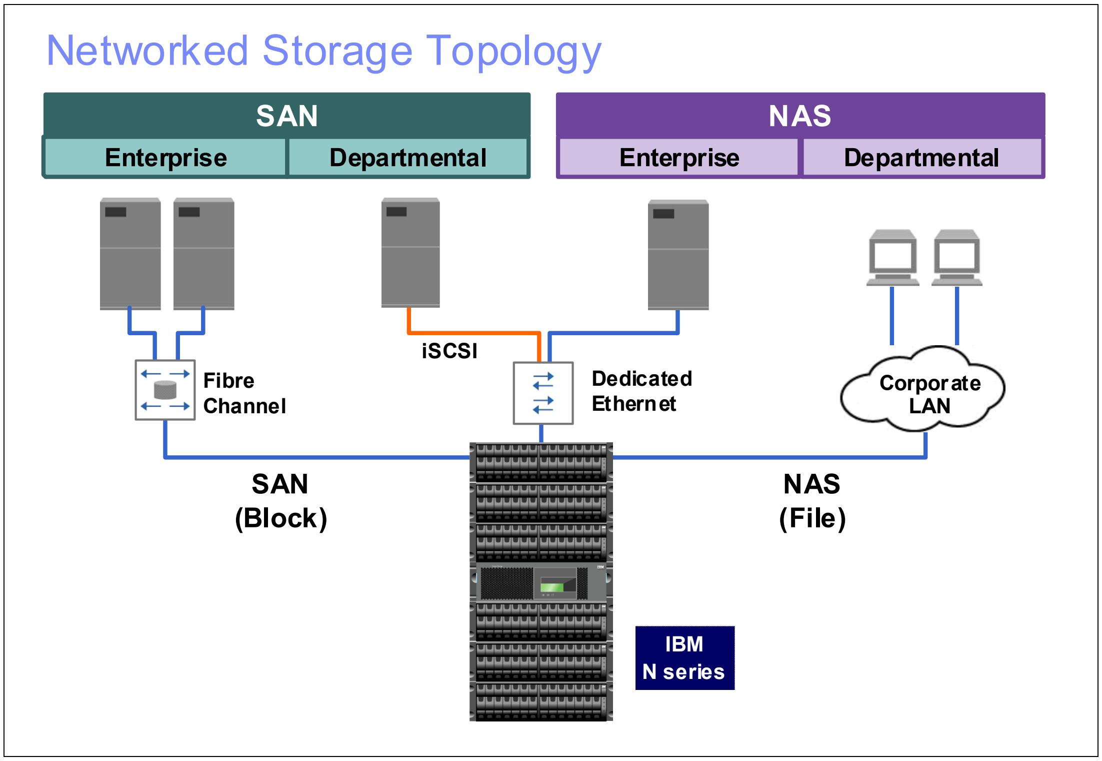


Figure 2-2 Multiprotocol N series

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.

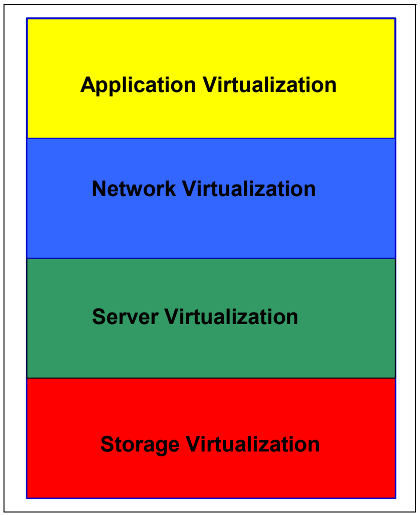


Figure 2-3 Virtualization stack

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.

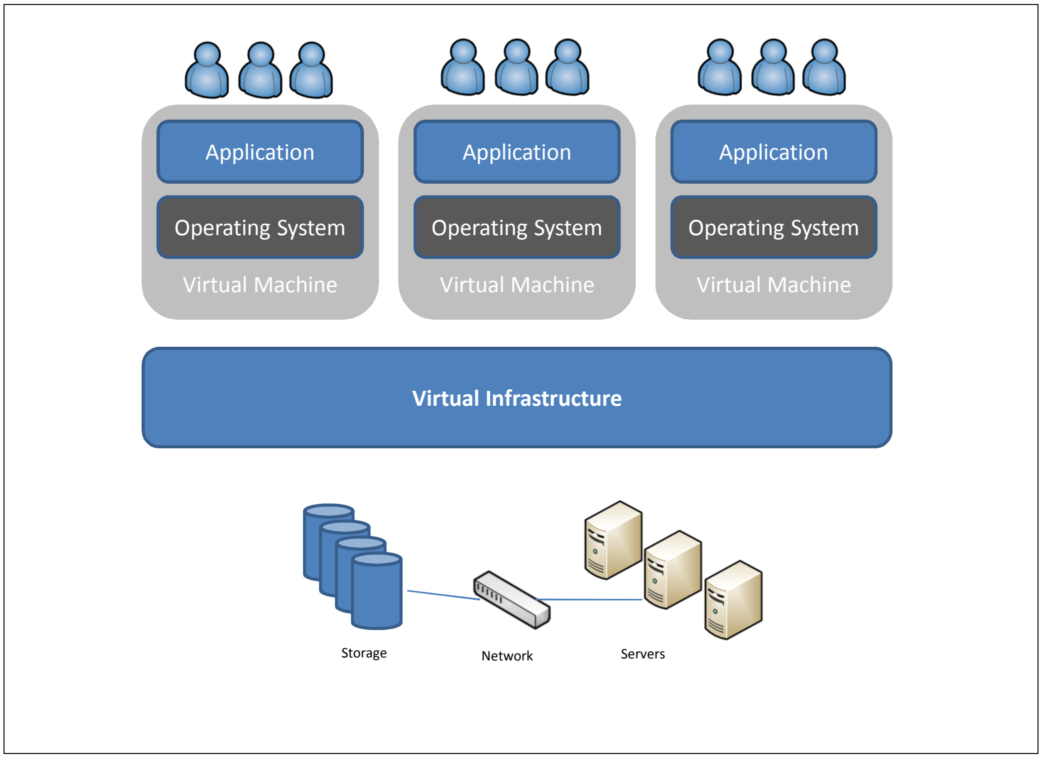


Figure 2-4 Server virtualization

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 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).

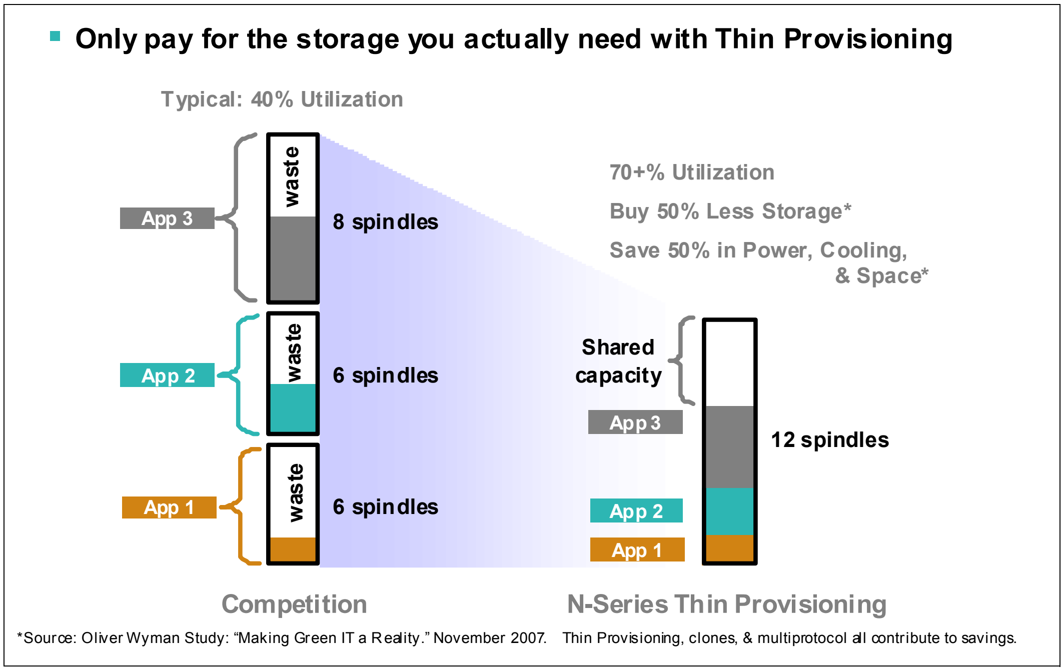

Only pay for the storage you actually need with Thin Provisioning
Typical: 40% Utilization
App 3
waste
8 spindles
App 2
waste
6 spindles
App 1
waste
6 spindles
70+% Utilization
Buy 50% Less Storage*
Save 50% in Power, Cooling, & Space*
Shared capacity
App 3
App 2
App 1
12 spindles
Competition
N-Series Thin Provisioning
*Source: Oliver Wyman Study: "Making Green IT a Reality." November 2007.
Thin Provisioning, clones, & multiprotocol all contribute to savings.

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: 2 x IBM System Storage N series 6070
- 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 5.1
  - VMware vCenter 5.1

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

Figure 2-6 shows the environment used to write this book.

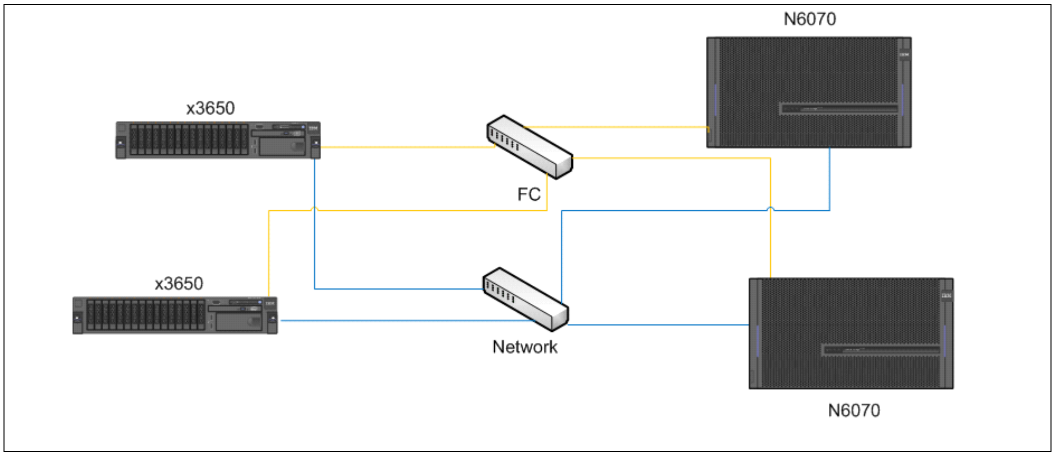


Figure 2-6 The environment used to write this book

3

Benefits of N series with VMware vSphere 5.1

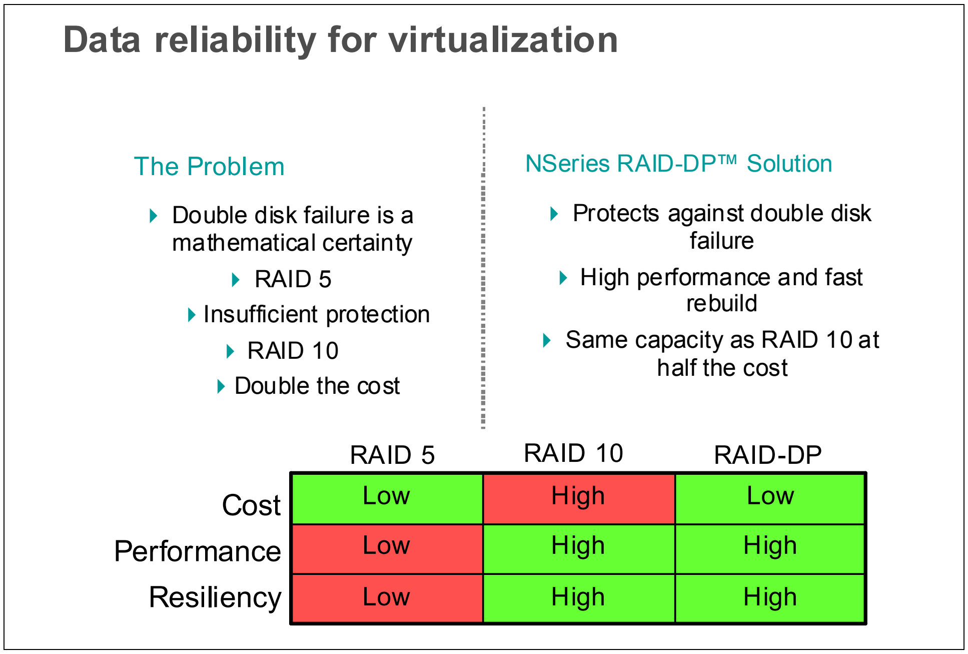
This chapter outlines the benefits that the IBM System Storage N series provides to VMware vSphere 5.1 environments. It includes the following topics:

- 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

© Copyright IBM Corp. 2013. All rights reserved.

3.1 Increased protection with RAID-DP

In a VWware vSphere 5.x environment, the performance and availability of the storage system are important. With a number of servers systems being consolidated into each VMware host, 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.



Data reliability for virtualization

The Problem

- Double disk failure is a mathematical certainty
  - RAID 5
    - Insufficient protection
  - RAID 10
    - Double the cost

NSeries RAID-DP™ Solution

- Protects against double disk failure
- High performance and fast rebuild
- Same capacity as RAID 10 at half the cost

	RAID 5	RAID 10	RAID-DP
Cost	Low	High	Low
Performance	Low	High	High
Resiliency	Low	High	High

Figure 3-1 RAID-DP

3.2 Cloning virtual machines

Although guests clone can be performed natively with VMware, combining it with the cloning features from N series provides significant storage space savings. This type of cloning is particularly helpful when testing existing VMs. Guests can be cloned at the N series level using little additional disk capacity due to the deduplication, explained on 3.9, “Using N series deduplication with VMware”, where VMware guest cloning alone would take double of 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.

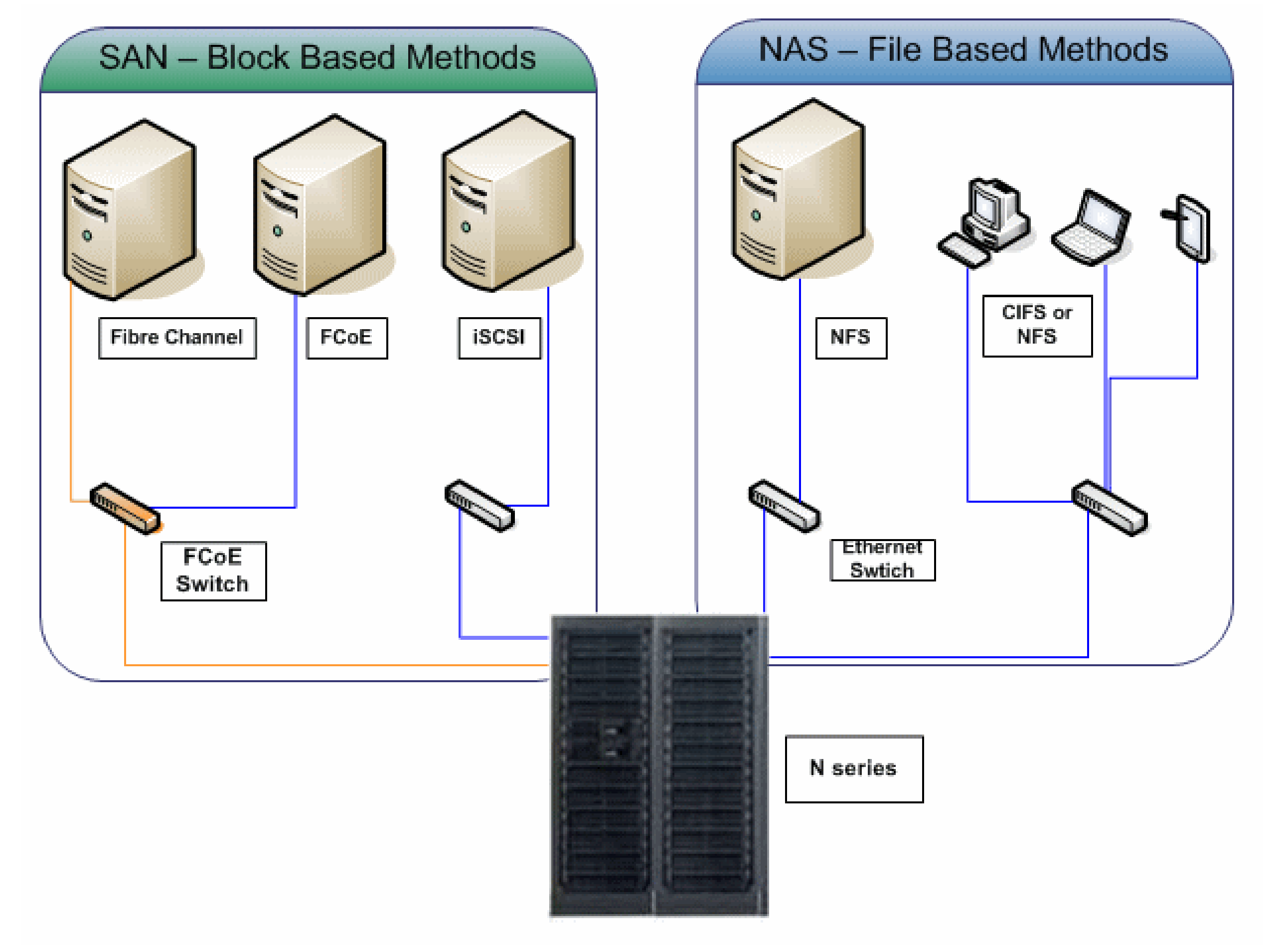


Figure 3-2 Storage protocols used by VMWare and available on N series family

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 through the usage of these methods:

- Snapshot of a logical unit number (LUN), to be restored later. Snapshots can be used to restore data in a case of a storage failure or corrupted file systems.
- FlexClone, which enables the clone of a LUN to make it available to another 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.

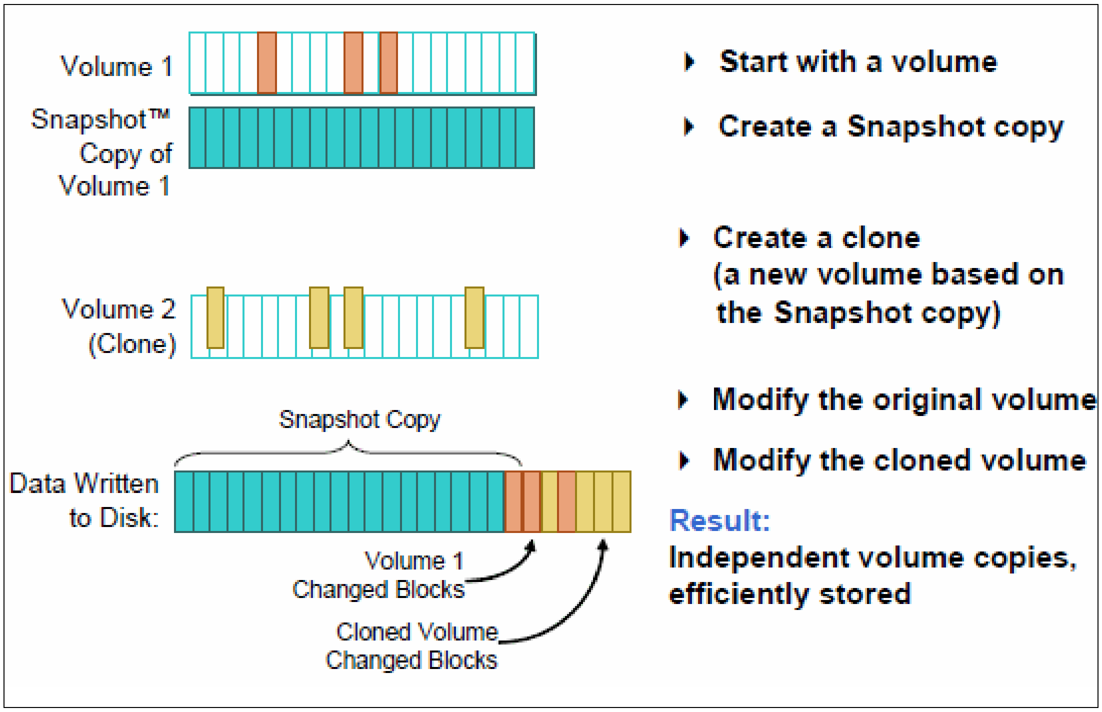

Volume 1
Snapshot™ Copy of Volume 1
Volume 2 (Clone)
Snapshot Copy
Data Written to Disk:
Volume 1 Changed Blocks
Cloned Volume Changed Blocks
Start with a volume
Create a Snapshot copy
Create a clone (a new volume based on the Snapshot copy)
Modify the original volume
Modify the cloned volume
Result:
Independent volume copies, efficiently stored

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 where the FlexClone was taken.

3.5 N series LUNs for VMFS datastores

Adding as many hard drives as possible on the aggregates provide improved performance for LUNs residing on 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 are good criteria when deciding which servers should share the same datastores. Consider to have very important servers on their own datastore, on a single LUN from a single volume, so you can take full advantage of N series advanced functionalities, which are implemented at 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
- Redo log tracking for a mapped device
- Virtual machine migration with vMotion
- SAN management within a virtual machine

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

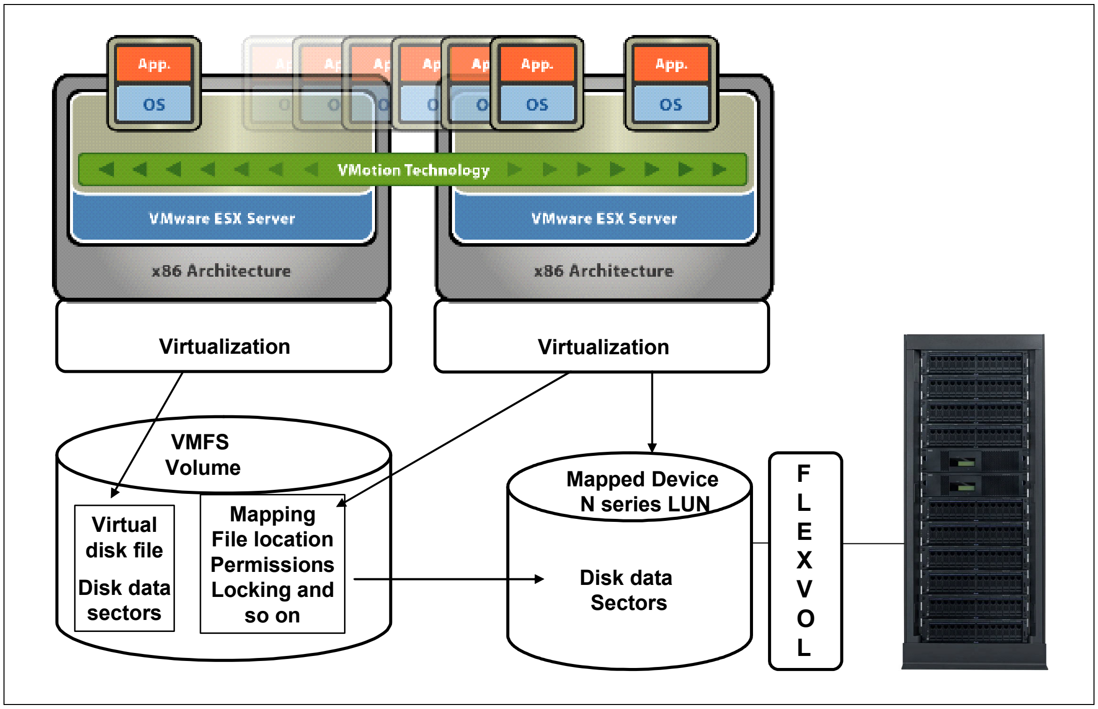


Figure 3-4 Mapping file data

3.7 Growing VMFS datastores

Starting with VMware vSphere version 4 and later versions, datastores can be easily extended by increasing the size of the N series LUN, and then adding that space to the datastore. Previous versions required to have a new LUN assigned to that datastore, creating an extent for it and making it hard to maintain.

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 current volume is quickly replaced by the Snapshot one. 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 VM can be created from that Snapshot can be created and just the required files can be copied back manually.
- If backup is performed 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, allowing for space usage savings on the storage and creating an unified backup and restore plan.

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, and using a pointer to refer to it on the next occurrences, 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, which 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.

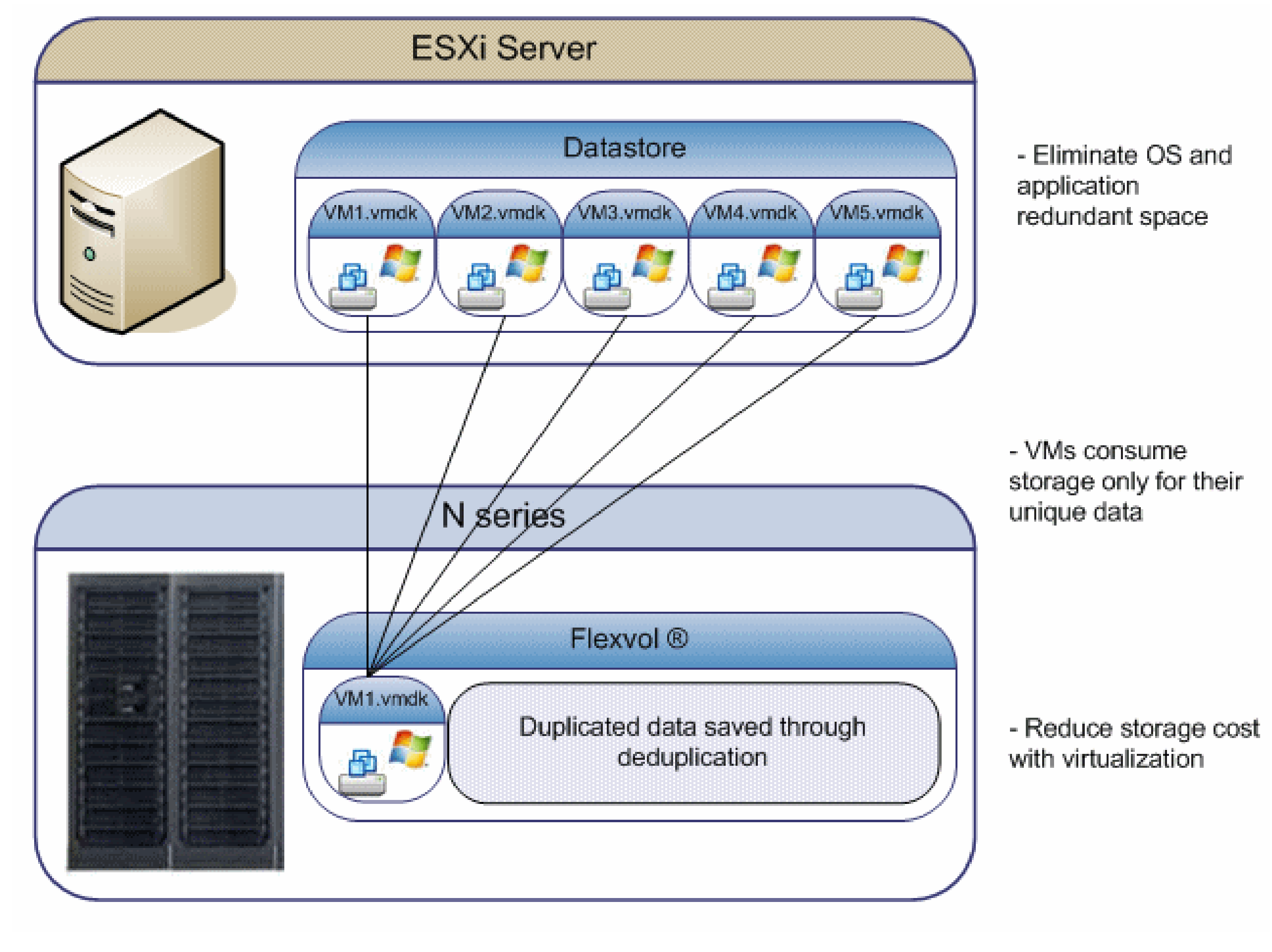

ESXi Server
Datastore
VM1.vmdk
VM2.vmdk
VM3.vmdk
VM4.vmdk
VM5.vmdk
- Eliminate OS and application redundant space
- VMs consume storage only for their unique data
N series
Flexvol ®
VM1.vmdk
Duplicated data saved through deduplication
- Reduce storage cost with virtualization

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 be manage, power, and cool. Similar to server virtualization, IBM Real-time Compression fits seamlessly into your storage infrastructure, without requiring changes to management 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 has the following benefits:

- 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 on following gains:
  - Up to 80% of data footprint reduction
  - 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, replication, and backup and restore-related operations all benefit from the data reduction and perform better.
- Transparency: No configuration change is 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 less than 30 minutes.

For more details on integration of vSphere 5.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 N series and VMware vSphere 5.1

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

© Copyright IBM Corp. 2013. All rights reserved.

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 that 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, this book provides 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 Interoperability Matrix” 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:

`http://www-01.ibm.com/support/docview.wss?uid=ssg1S7003278`

4.1.3 VMware vSphere 5.1

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/vsphere5/r51/vsphere-51-configuration-maximums.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. It 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 ESXi 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 need to be clustered and using RAID-DP. For even higher availability and redundancy, use an N series MetroCluster as a foundation for VMware vSphere solutions (Figure 4-1).

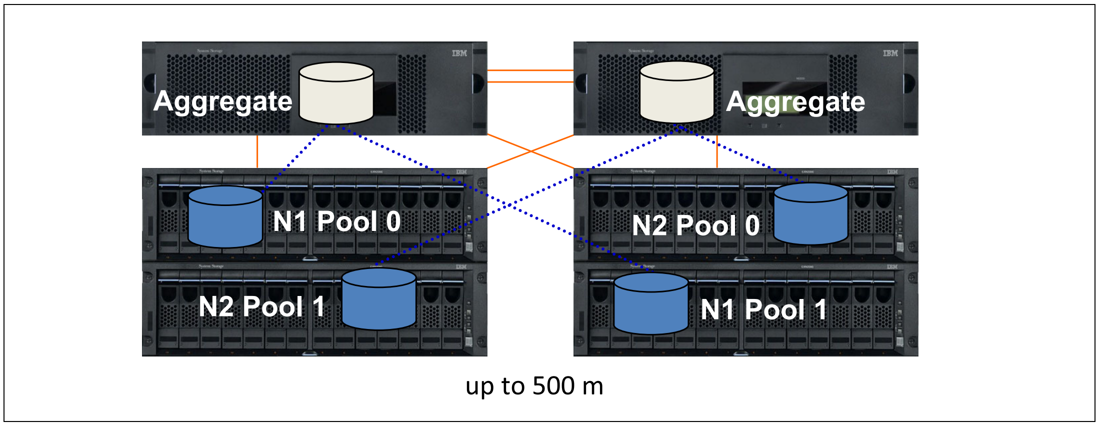


Figure 4-1 N series MetroCluster protection

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 section 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 5.1. 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. It is the most common method for deploying storage in VMware environments (see Figure 4-2).

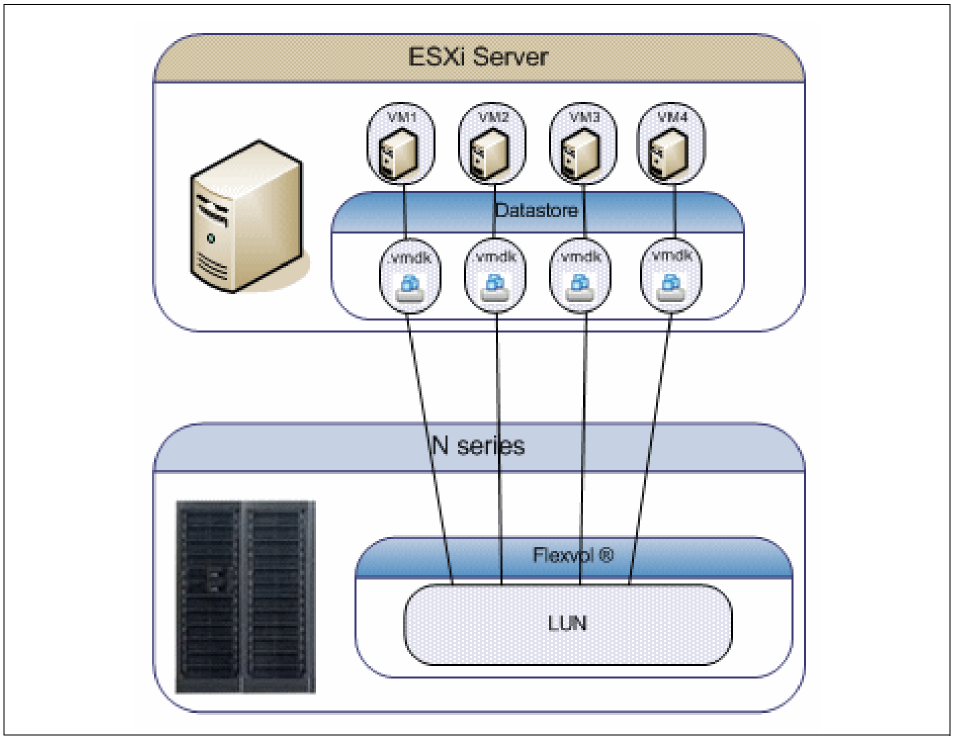


Figure 4-2 VMFS datastore: Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), iSCSI

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 address:

http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-storage-guide.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. They 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.

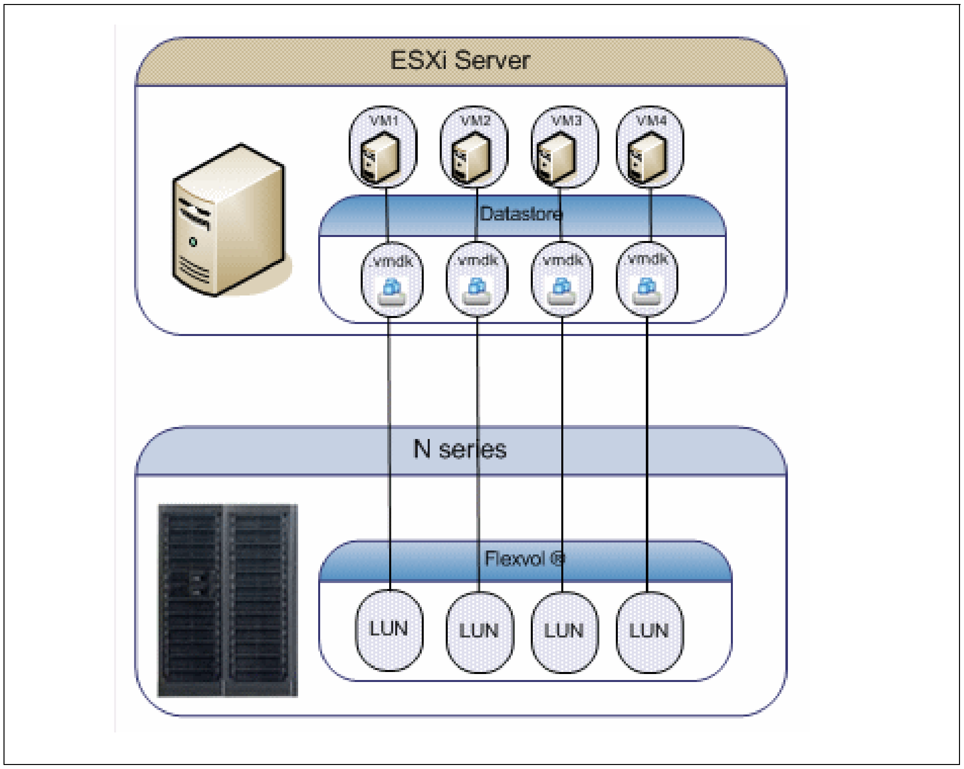


Figure 4-3 RDM access of LUNs by guests

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

`http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-storage-guide.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 ESXi 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. They 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.

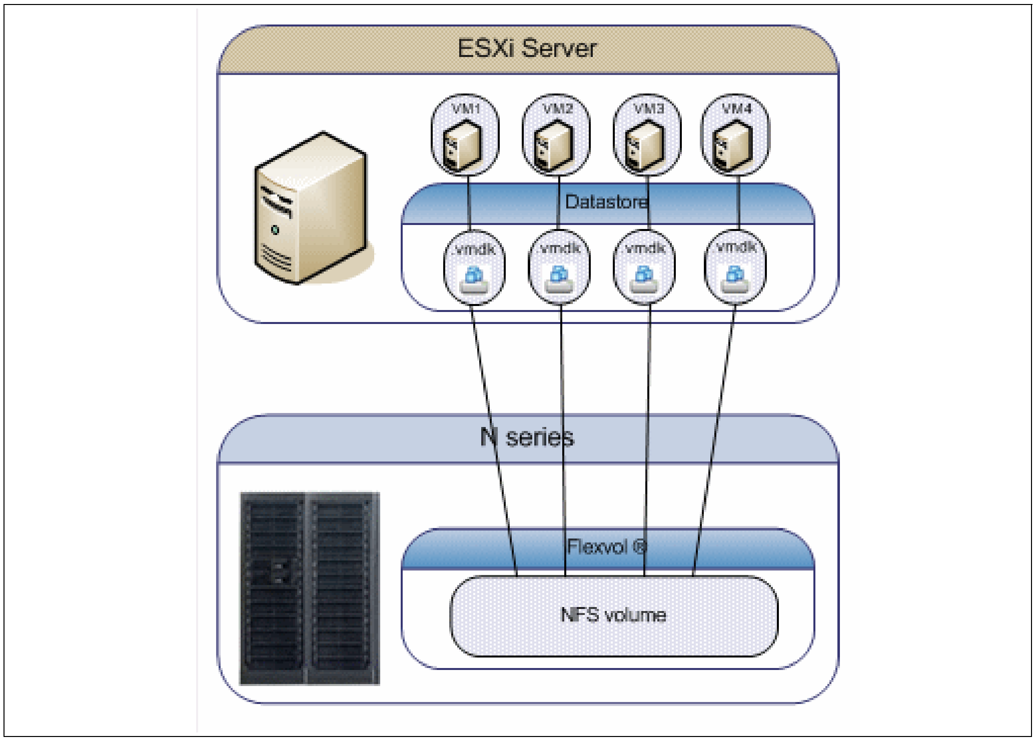


Figure 4-4 NFS accessed datastore

> **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.

For more information about storing .vmdk files on NFS, see the *vCenter Server and Host Management* at the following website:

http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-host-management-guide.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

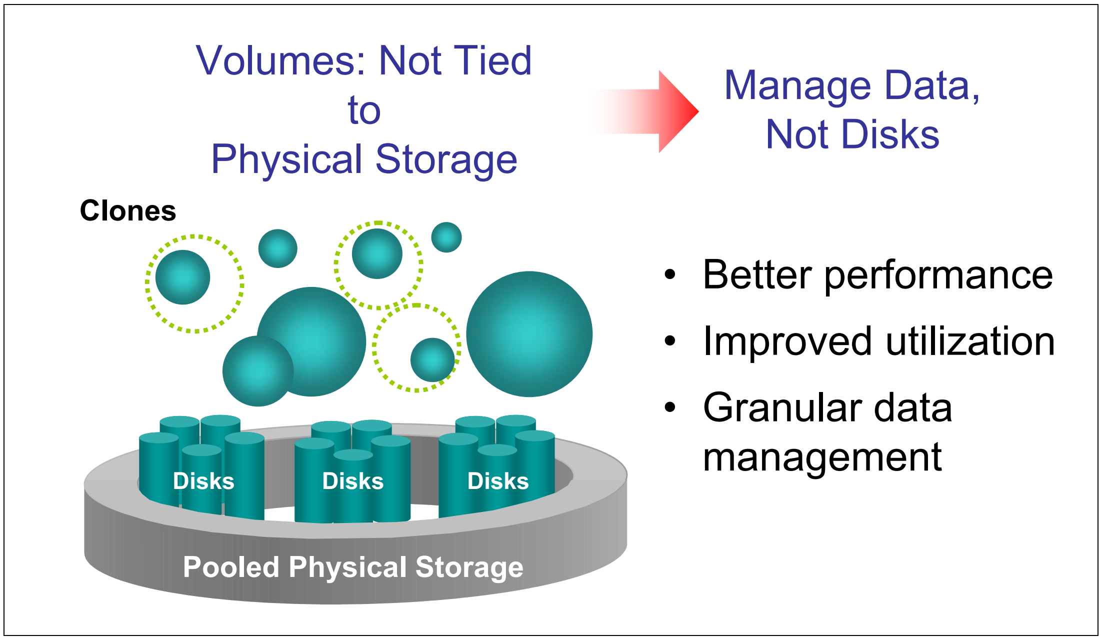
An aggregate is the virtualization layer of Data ONTAP that abstracts physical disks from logical data sets, which are referred to as *flexible volumes*. Aggregates provide a means where the total IOPS available to all of the physical disks is pooled as a resource. This design is better suited to meet 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 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 ESXi 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. It is because Data ONTAP implements these storage-side features at the flexible volume level.



Volumes: Not Tied to Physical Storage

Manage Data, Not Disks

- Better performance
- Improved utilization
- Granular data management

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 section.

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 5.1 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 64 TB for vSphere 5.x. However, the N series system maximum LUN size is 16 TB.

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

http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-storage-guide.pdf

4.5 Storage connectivity

This section 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.

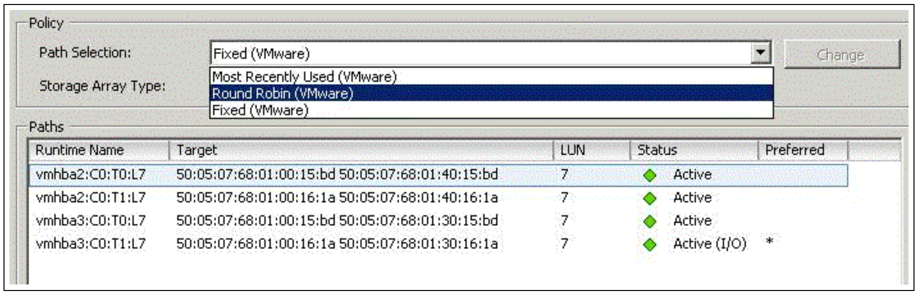
Fibre Channel multipathing

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 fully supported at that time.

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

VMware ESXi 5.1 supports ALUA as multipath policy, which is implemented by selecting Round Robin as the Storage Array Type, as shown in Figure 4-6.



Path Selection: Fixed (VMware)

Storage Array Type:

Runtime Name	Target	LUN	Status	Preferred
vmhba2:C0:T0:L7	50:05:07:68:01:00:15:bd 50:05:07:68:01:40:15:bd	7	🟩 Active	
vmhba2:C0:T1:L7	50:05:07:68:01:00:16:1a 50:05:07:68:01:40:16:1a	7	🟩 Active	
vmhba3:C0:T0:L7	50:05:07:68:01:00:15:bd 50:05:07:68:01:30:15:bd	7	🟩 Active	
vmhba3:C0:T1:L7	50:05:07:68:01:00:16:1a 50:05:07:68:01:30:16:1a	7	🟩 Active (I/O)	*

Figure 4-6 Configuring VMware ESXi 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 ESXi Server FCP configurations, see the *IBM System Storage N series Interoperability Matrix* at the following website:

http://www-01.ibm.com/support/docview.wss?uid=ssg1S7003897

> **Access to IBM Systems support:** You must register for access to IBM Systems support applications and content. You can register at the following address:
>
> http://www-01.ibm.com/support/docview.wss?uid=ssg1S7003278

Verifying cfmode

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 ESXi Server.

For more information about the different cfmodes available and the impact of changing a cfmode, see the *Data ONTAP 8.1.x Block Access Management Guide for iSCSI and FCP* at this website:

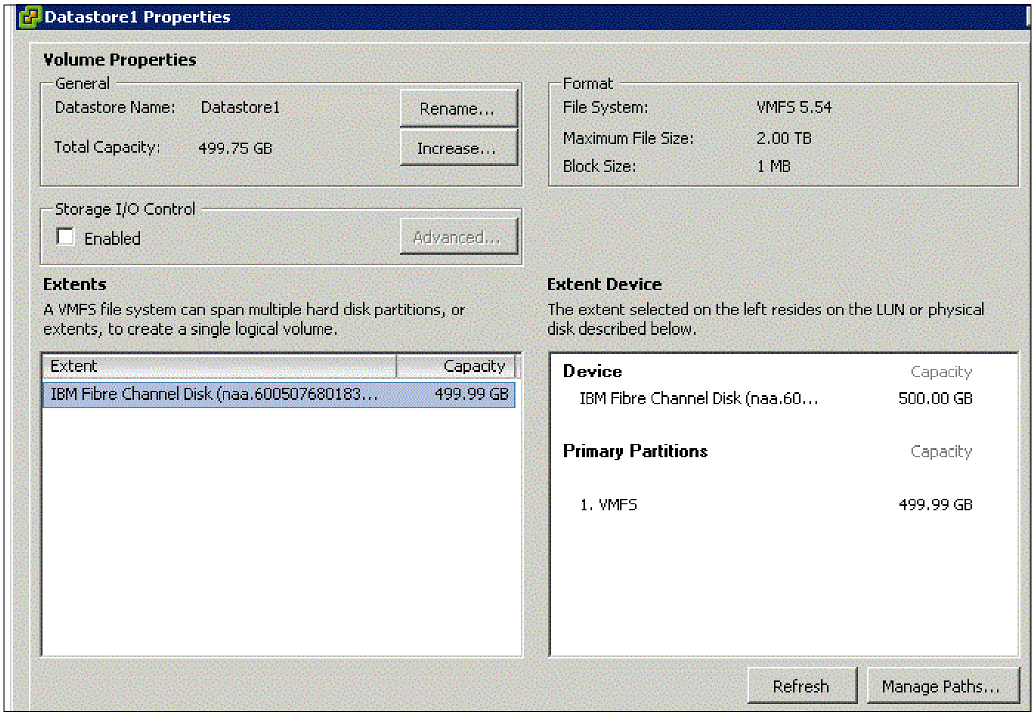
https://library.netapp.com/ecmdocs/ECMM1277837/html/bsag/frameset.html

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).



Volume Properties

General
Datastore Name: Datastore1
Total Capacity: 499.75 GB

Format
File System: VMFS 5.54
Maximum File Size: 2.00 TB
Block Size: 1 MB

Storage I/O Control
☐ Enabled

Extents
A VMFS file system can span multiple hard disk partitions, or extents, to create a single logical volume.

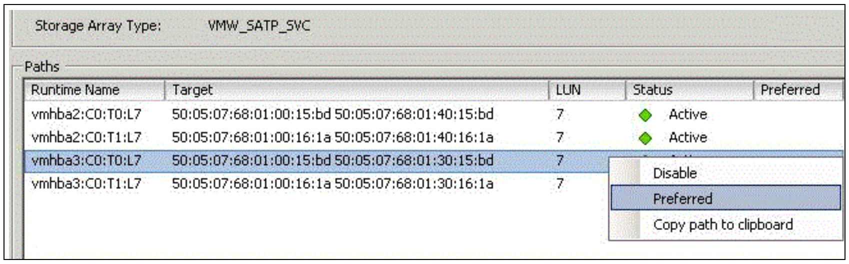
Extent	Capacity
IBM Fibre Channel Disk (naa.600507680183...	499.99 GB

Extent Device
The extent selected on the left resides on the LUN or physical disk described below.

Device	Capacity
IBM Fibre Channel Disk (naa.60...	500.00 GB
Primary Partitions	Capacity
1. VMFS	499.99 GB

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.



Storage Array Type: VMW_SATP_SVC

Paths

Runtime Name	Target	LUN	Status	Preferred
vmhba2:C0:T0:L7	50:05:07:68:01:00:15:bd 50:05:07:68:01:40:15:bd	7	◆ Active	
vmhba2:C0:T1:L7	50:05:07:68:01:00:16:1a 50:05:07:68:01:40:16:1a	7	◆ Active	
vmhba3:C0:T0:L7	50:05:07:68:01:00:15:bd 50:05:07:68:01:30:15:bd	7	Active	
vmhba3:C0:T1:L7	50:05:07:68:01:00:16:1a 50:05:07:68:01:30:16:1a	7		

Figure 4-8 Changing the Preferred path

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.

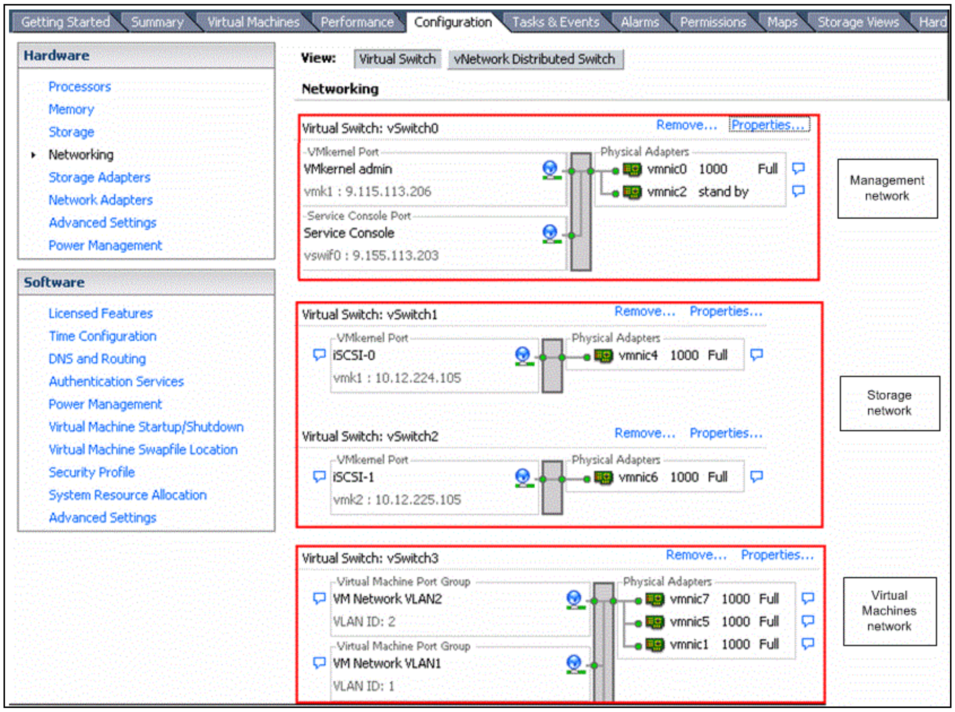
Hardware initiator Uses a dedicated iSCSI HBA to establish communication with the target system. By using this type of iSCSI initiator, you can take advantage of using boot from SAN because the communication can be initiated by the firmware of the iSCSI HBA.

iSCSI security

The most recent version of the iSCSI protocol supports both Encryption through IPSec and IKE, and Authentication through a variety of methods. They 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.

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



Virtual Switch: vSwitch0
VMkernel Port: VMkernel admin, vmk1 : 9.115.113.206
Service Console Port: Service Console, vswif0 : 9.155.113.203
Physical Adapters: vmnic0 1000 Full; vmnic2 stand by

Virtual Switch: vSwitch1
VMkernel Port: iSCSI-0, vmk1 : 10.12.224.105
Physical Adapters: vmnic4 1000 Full

Virtual Switch: vSwitch2
VMkernel Port: iSCSI-1, vmk2 : 10.12.225.105
Physical Adapters: vmnic6 1000 Full

Virtual Switch: vSwitch3
Virtual Machine Port Group: VM Network VLAN2, VLAN ID: 2
Virtual Machine Port Group: VM Network VLAN1, VLAN ID: 1
Physical Adapters: vmnic7 1000 Full; vmnic5 1000 Full; vmnic1 1000 Full

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 ESXi 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 ESXi Server I/O Compatibility Guide* at the following web page to verify support for your hardware:

http://www.vmware.com/resources/compatibility/pdf/vi_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 5.1

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

http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-storage-guide.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 ESXi 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 ESXi Servers and multiple datastores with stacked switches.

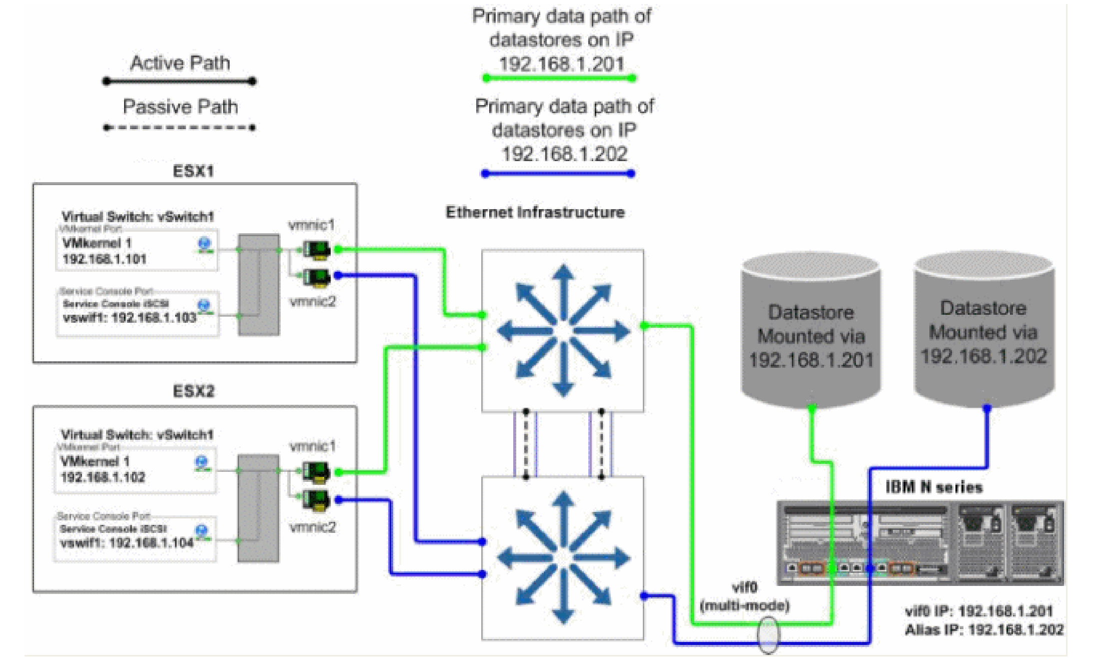


Figure 4-10 Datastore connections with a stacked switch configuration

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

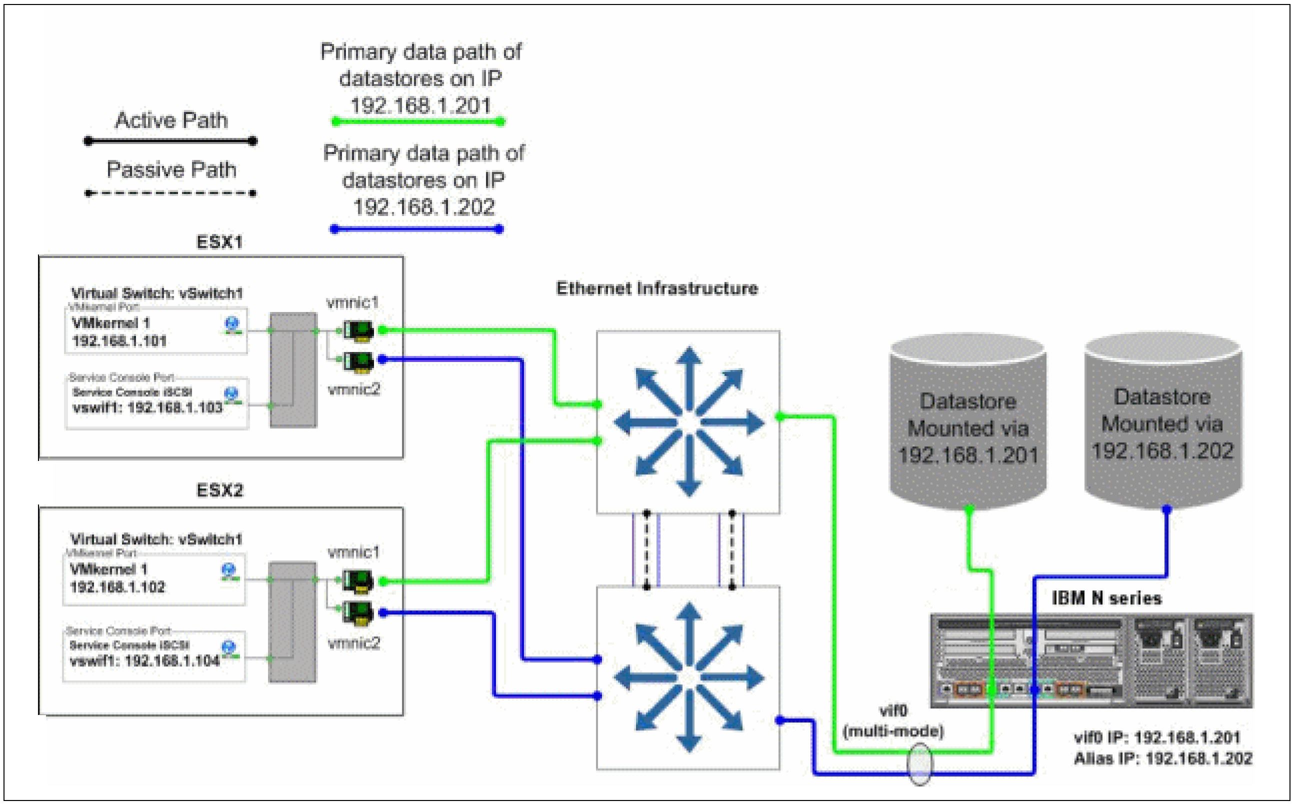


Figure 4-11 Datastore connections with a non-stacked switch configuration

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.

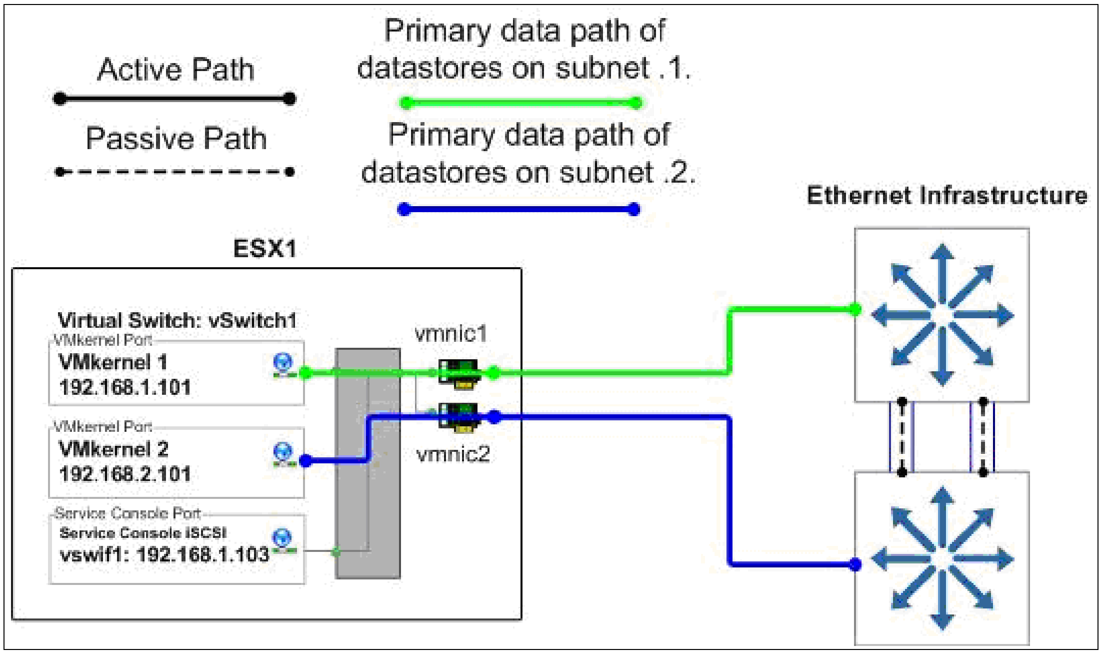


Figure 4-12 VMware ESXi Server Switch1 normal operation

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

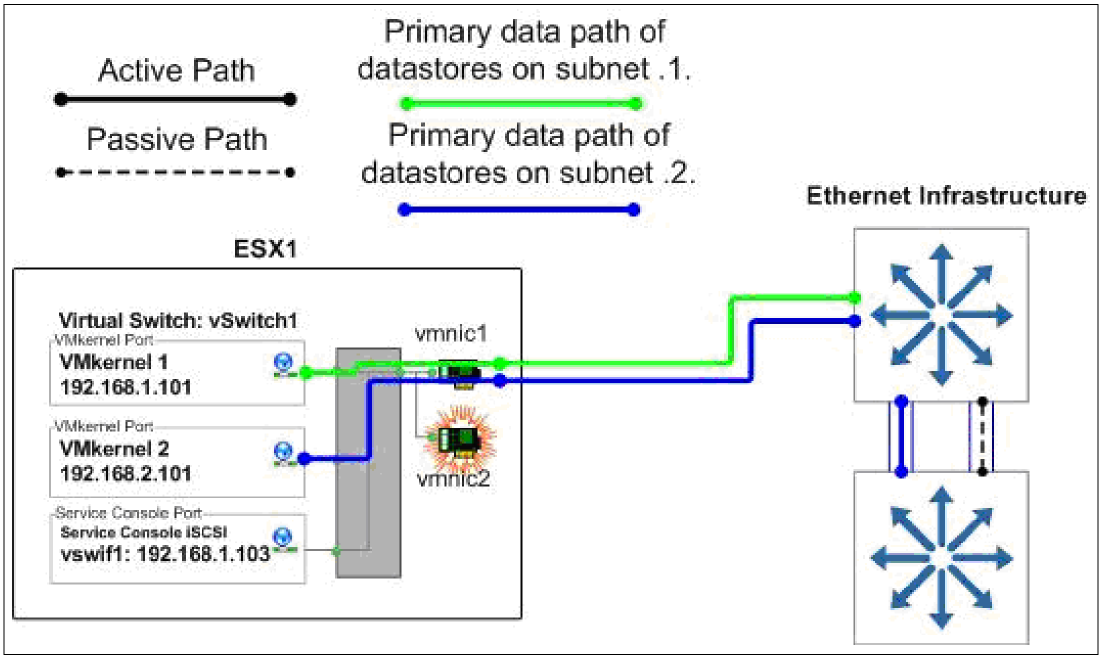


Figure 4-13 VMware ESXi Server Switch1 unavailable operation

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.

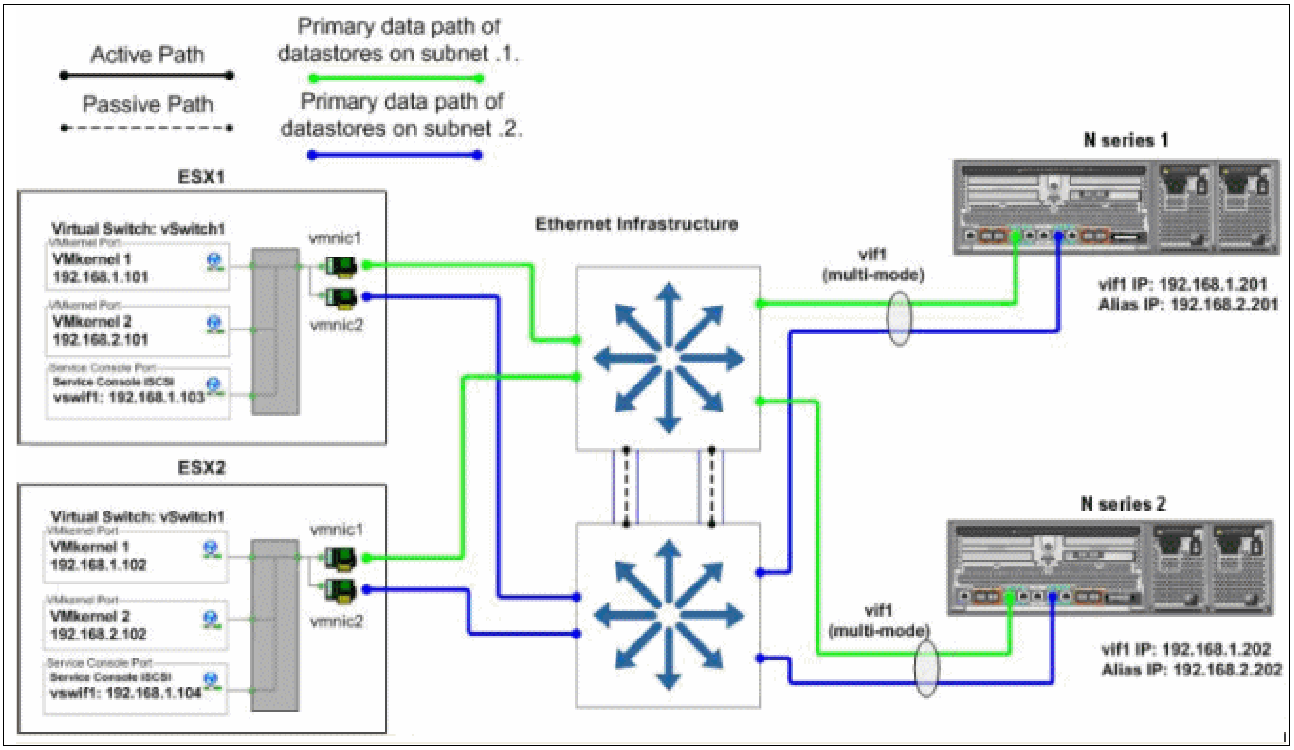


Figure 4-14 Storage-side multimode VIFs using LACP across stacked switches

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.

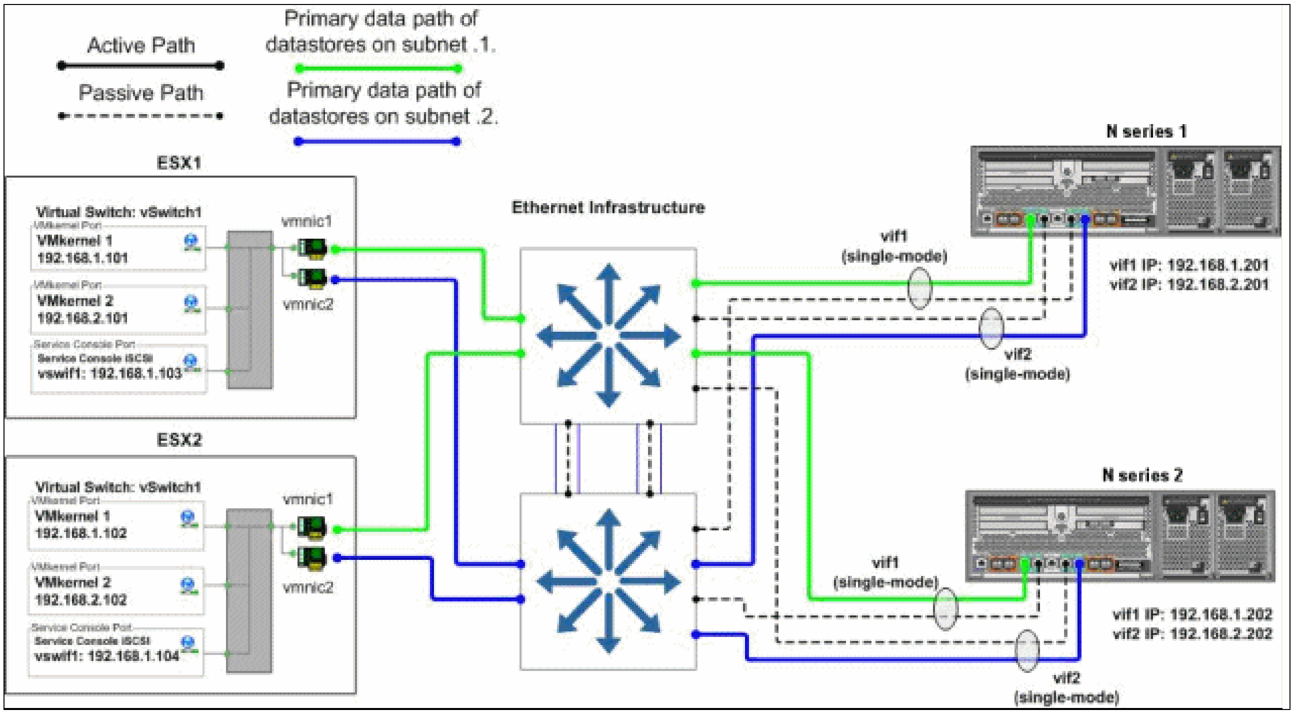


Figure 4-15 Storage-side single mode VIFs

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.

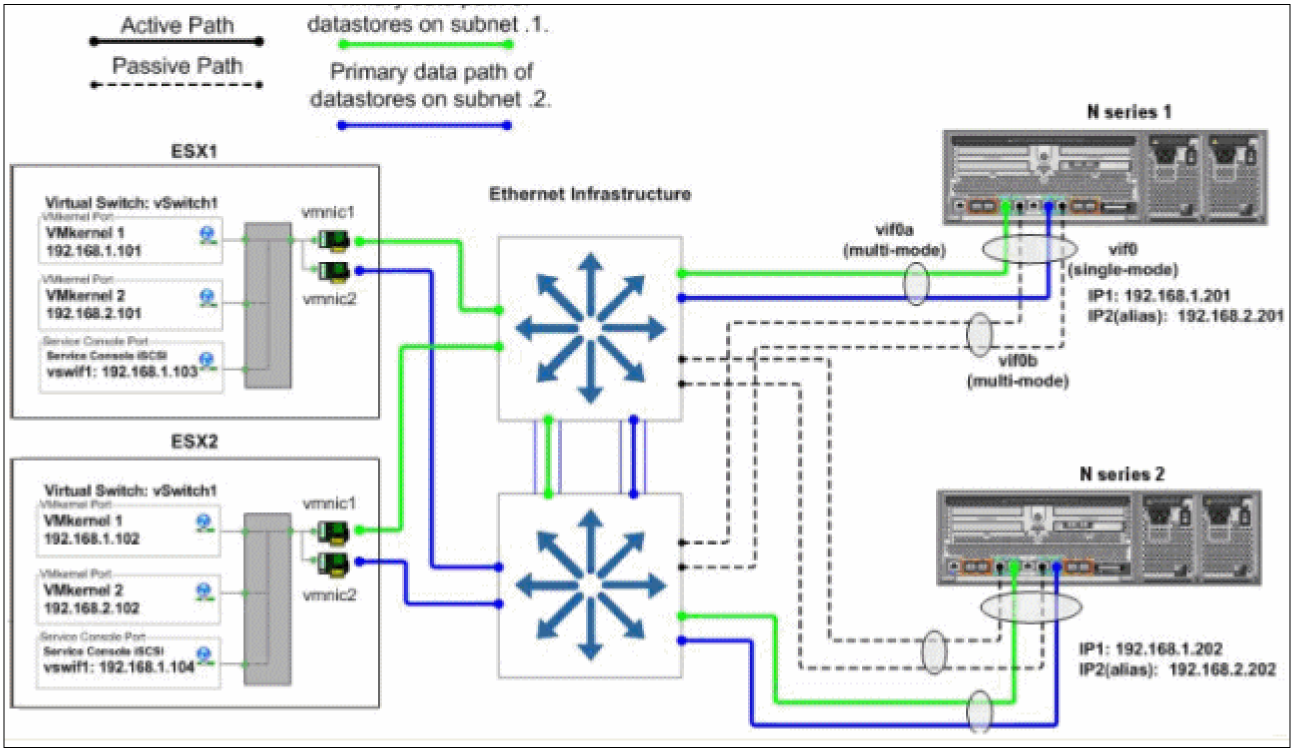


Figure 4-16 Storage-side multimode VIFs

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 ESXi 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 ESXi 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 ESXi 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 section provides information about the backup and recovery techniques and technologies that you can use with a VMware vSphere 5.1 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://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-virtual-machine-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 5.1 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).

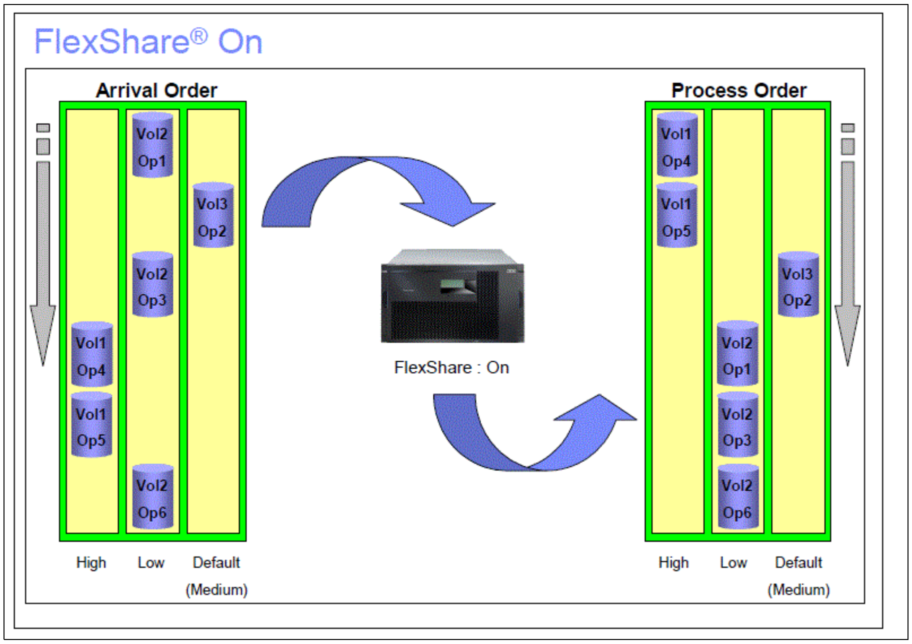


Figure 4-17 FlexShare prioritization

FlexShare is supported on N series storage systems running Data ONTAP Version 8.1 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 section 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:

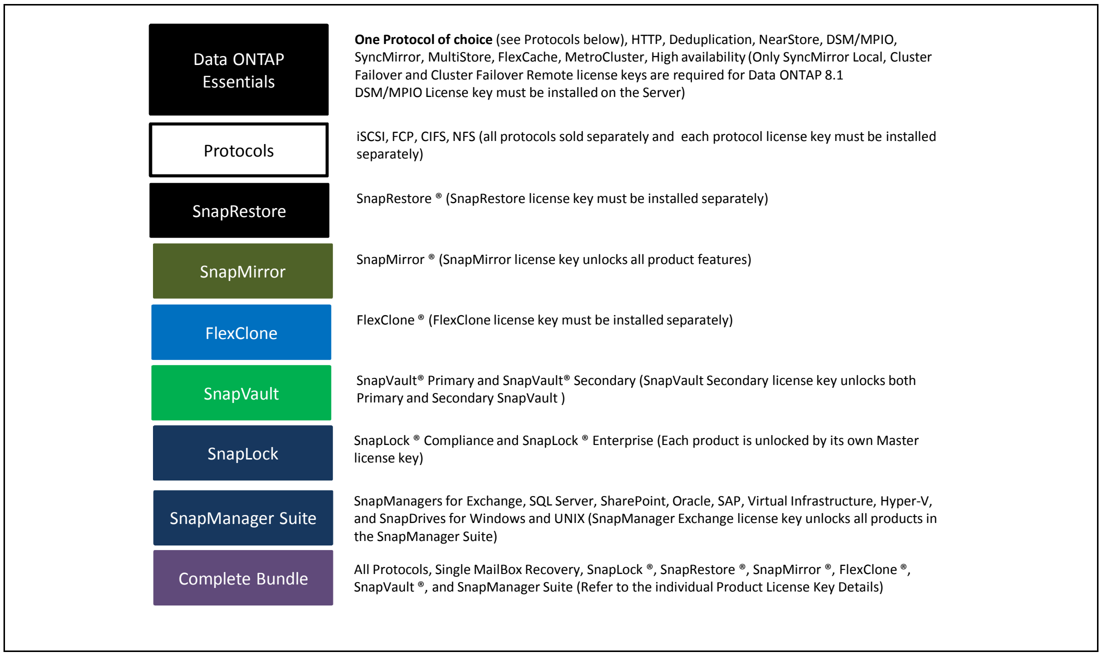
- VCenter Agent for ESXi Server
- VMotion
- VMware High Availability
- VMware Dynamic Resource Scheduling
- VMware Consolidated Backup
- VMware Fault Tolerance.

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.



Data ONTAP Essentials	**One Protocol of choice** (see Protocols below), HTTP, Deduplication, NearStore, DSM/MPIO, SyncMirror, MultiStore, FlexCache, MetroCluster, High availability (Only SyncMirror Local, Cluster Failover and Cluster Failover Remote license keys are required for Data ONTAP 8.1 DSM/MPIO License key must be installed on the Server)
Protocols	iSCSI, FCP, CIFS, NFS (all protocols sold separately and each protocol license key must be installed separately)
SnapRestore	SnapRestore ® (SnapRestore license key must be installed separately)
SnapMirror	SnapMirror ® (SnapMirror license key unlocks all product features)
FlexClone	FlexClone ® (FlexClone license key must be installed separately)
SnapVault	SnapVault® Primary and SnapVault® Secondary (SnapVault Secondary license key unlocks both Primary and Secondary SnapVault)
SnapLock	SnapLock ® Compliance and SnapLock ® Enterprise (Each product is unlocked by its own Master license key)
SnapManager Suite	SnapManagers for Exchange, SQL Server, SharePoint, Oracle, SAP, Virtual Infrastructure, Hyper-V, and SnapDrives for Windows and UNIX (SnapManager Exchange license key unlocks all products in the SnapManager Suite)
Complete Bundle	All Protocols, Single MailBox Recovery, SnapLock ®, SnapRestore ®, SnapMirror ®, FlexClone ®, SnapVault ®, and SnapManager Suite (Refer to the individual Product License Key Details)

Figure 4-18 N series software structure

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

> **Additional information:** For further information regarding N series licensing, see the topic, “Using License Keys with Data ONTAP 8.1 7-Mode” at the following website:
>
> https://www-304.ibm.com/support/entdocview.wss?uid=ssg1S1003943

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 5.1 using N series storage

This chapter explains how to install and configure the VMware ESXi 5.1 operating system by using local disks on a server. It includes the following topics:

- Pre-installation tasks
- Installing the ESXi operating system

© Copyright IBM Corp. 2013. All rights reserved.

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.

In our scenario, we are installing ESXi 5.1 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 ESXi, 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 5.1 OS installation ISO from the VMware website:

  https://my.vmware.com/web/vmware/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/5_1

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, using these guidelines:

- 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 76.
   - 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

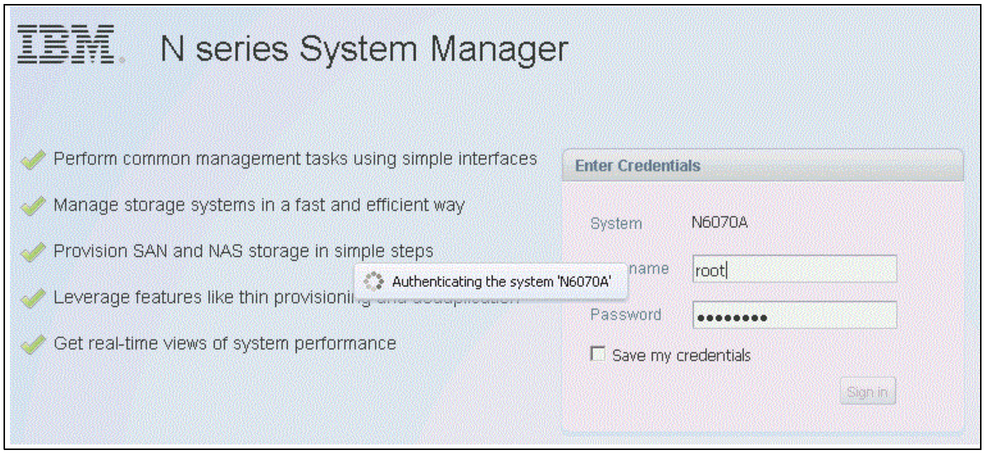
To set up a LUN in the N series to be used as a bootable LUN for the ESXi server:

1. Log in to the IBM N series System Manager:

   a. Launch an IBM N series System Manager 2.0 console.

> **Tip:** This step assumes that you have discovered and added your N series storages to the System Manager console.

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



IBM. N series System Manager

- Perform common management tasks using simple interfaces
- Manage storage systems in a fast and efficient way
- Provision SAN and NAS storage in simple steps
- Leverage features like thin provisioning and deduplication
- Get real-time views of system performance

Authenticating the system 'N6070A'

Enter Credentials

System N6070A

name root

Password ••••••••

□ Save my credentials

Figure 5-1 N series Overview authentication 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 5-2.

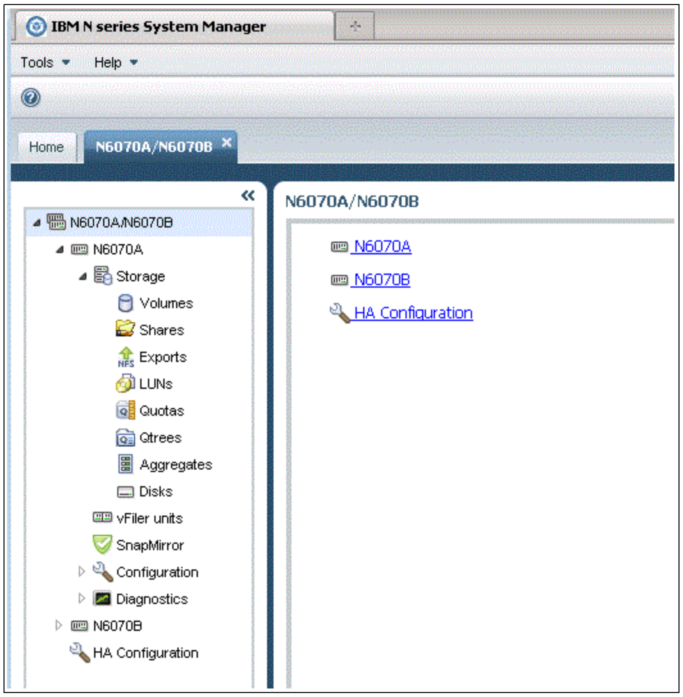


Figure 5-2 Main menu window

2. Create an aggregate:

   a. In the left pane, select **Aggregates** → **Create** (Figure 5-3).

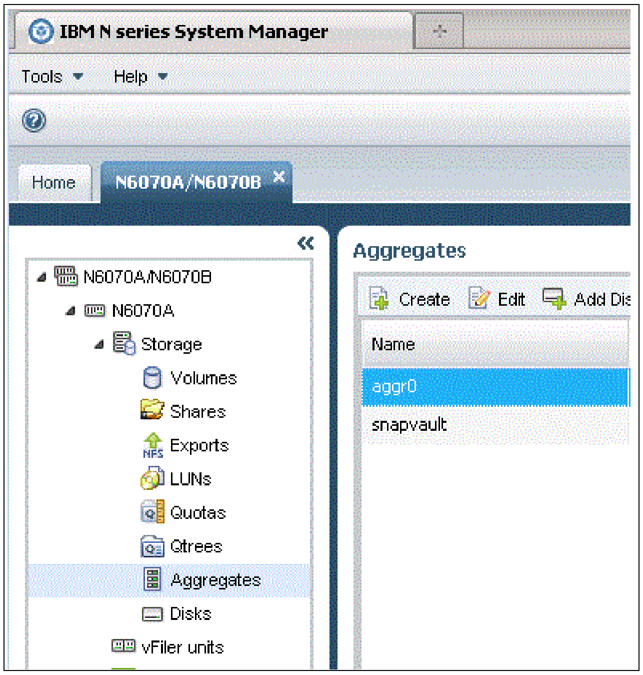
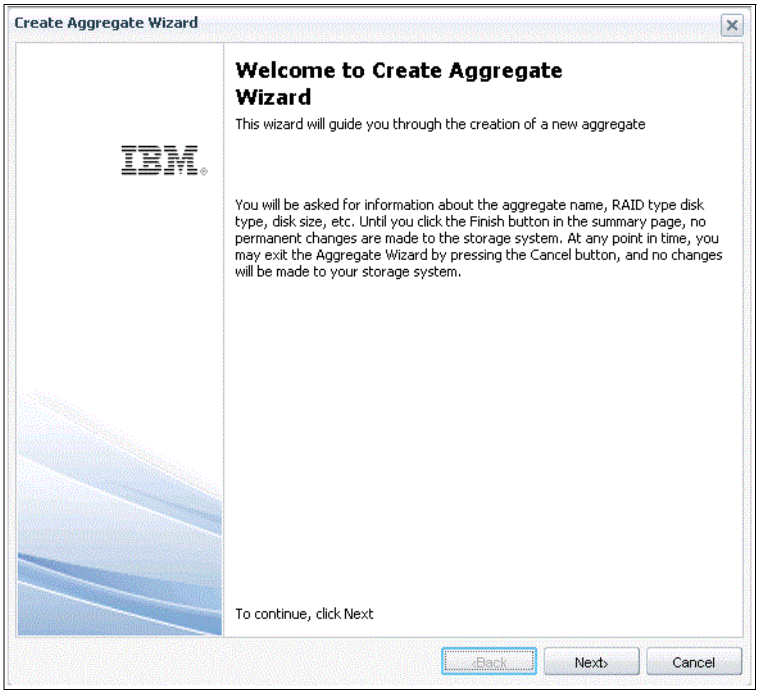


Figure 5-3 Selecting the option to create an aggregate

   b. In the Aggregate Wizard window (Figure 5-4), click **Next**.



Welcome to Create Aggregate Wizard

This wizard will guide you through the creation of a new aggregate

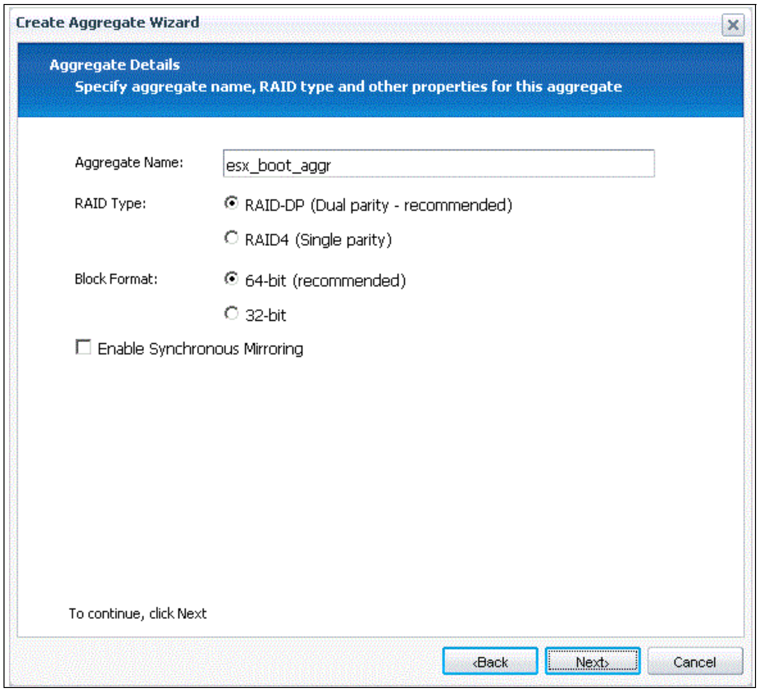
You will be asked for information about the aggregate name, RAID type disk type, disk size, etc. Until you click the Finish button in the summary page, no permanent changes are made to the storage system. At any point in time, you may exit the Aggregate Wizard by pressing the Cancel button, and no changes will be made to your storage system.

To continue, click Next

Figure 5-4 Aggregate Wizard Welcome window

   c. In the Aggregate Parameters panel (Figure 5-5), give the aggregate a name. In this example, we call it *esx_boot_aggr*. 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. With 64-bit block format, the 16 Tb size limitation is increased and the new maximums are defined by the storage system model.



Create Aggregate Wizard

Aggregate Details

Specify aggregate name, RAID type and other properties for this aggregate

Aggregate Name: esx_boot_aggr

RAID Type: ● RAID-DP (Dual parity - recommended) ○ RAID4 (Single parity)

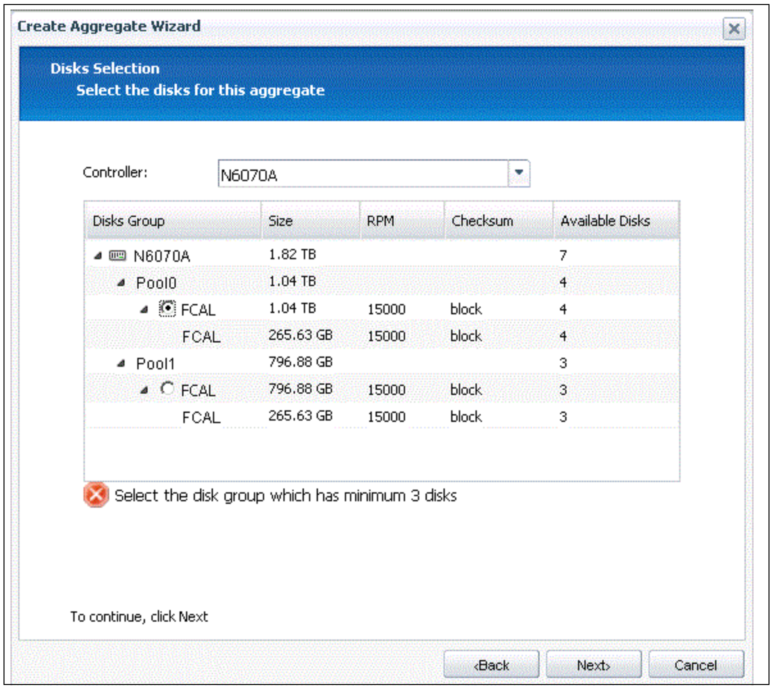
Block Format: ● 64-bit (recommended) ○ 32-bit

□ Enable Synchronous Mirroring

To continue, click Next

Figure 5-5 Naming the aggregate

d. In the Disk Selection panel (Figure 5-6), select which disk pool you want to use. Click **Next**.



Create Aggregate Wizard

Disks Selection

Select the disks for this aggregate

Controller: N6070A

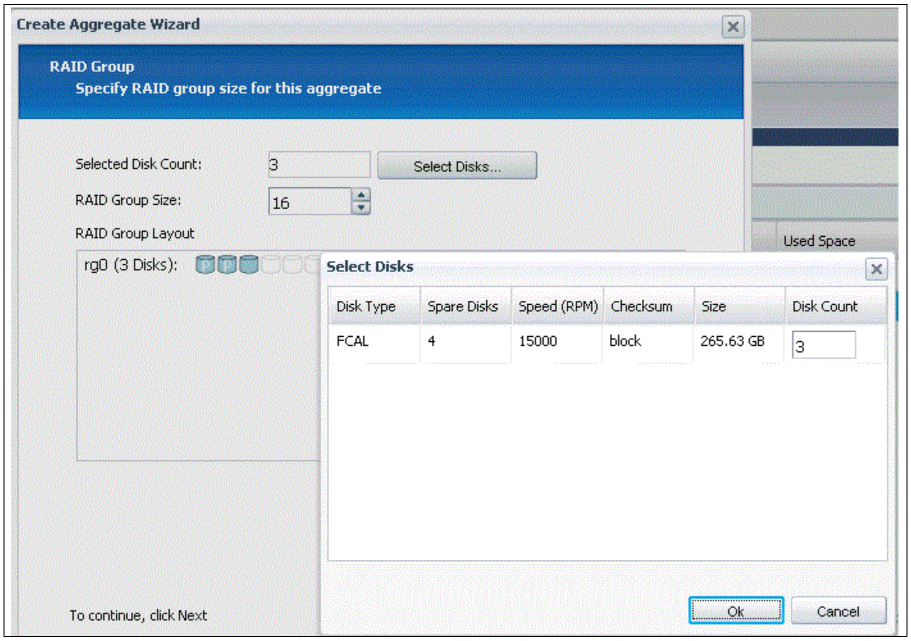
Disks Group	Size	RPM	Checksum	Available Disks
N6070A	1.82 TB			7
Pool0	1.04 TB			4
● FCAL	1.04 TB	15000	block	4
FCAL	265.63 GB	15000	block	4
Pool1	796.88 GB			3
○ FCAL	796.88 GB	15000	block	3
FCAL	265.63 GB	15000	block	3

Select the disk group which has minimum 3 disks

To continue, click Next

Figure 5-6 Selecting disk pool

e. In the RAID Group panel (Figure 5-7), select the number of disks and the RAID Group. Click **Next**.



RAID Group
Specify RAID group size for this aggregate

Selected Disk Count: 3

RAID Group Size: 16

RAID Group Layout

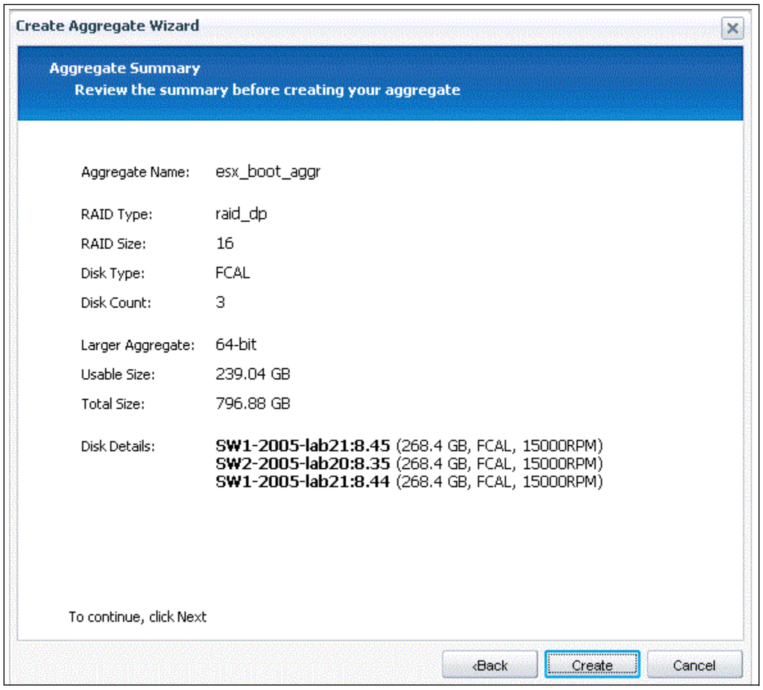
rg0 (3 Disks):

Disk Type	Spare Disks	Speed (RPM)	Checksum	Size	Disk Count
FCAL	4	15000	block	265.63 GB	3

To continue, click Next

Figure 5-7 Aggregate setup - disk selection

f. In the Commit panel (Figure 5-8), which summarizes the settings, click **Create**.



Aggregate Summary
Review the summary before creating your aggregate

Aggregate Name: esx_boot_aggr

RAID Type: raid_dp
RAID Size: 16
Disk Type: FCAL
Disk Count: 3

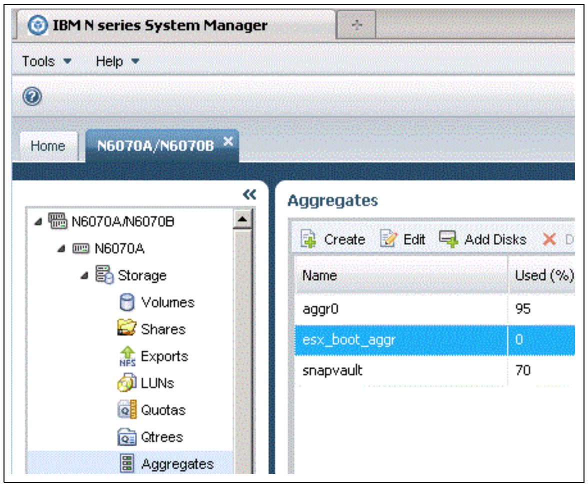
Larger Aggregate: 64-bit
Usable Size: 239.04 GB
Total Size: 796.88 GB

Disk Details:
SW1-2005-lab21:8.45 (268.4 GB, FCAL, 15000RPM)
SW2-2005-lab20:8.35 (268.4 GB, FCAL, 15000RPM)
SW1-2005-lab21:8.44 (268.4 GB, FCAL, 15000RPM)

To continue, click Next

Figure 5-8 Committing the aggregate setup

g. After the aggregate is created, in the left pane of the System Manager window (Figure 5-9), find the aggregate by selecting **Aggregate**.



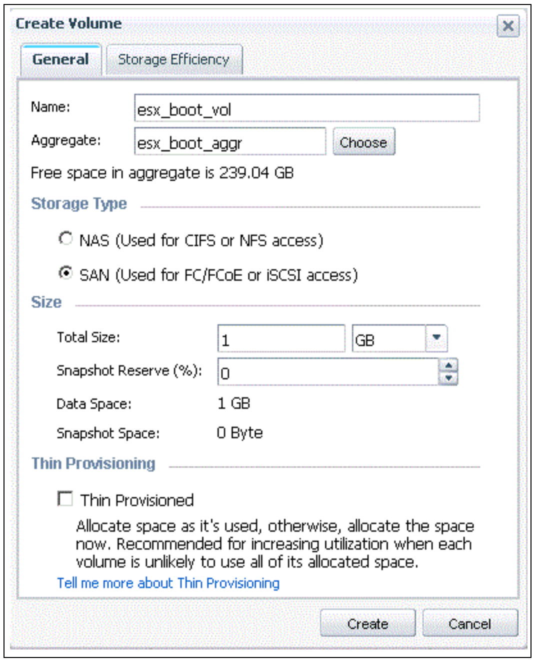
Name	Used (%)
aggr0	95
esx_boot_aggr	0
snapvault	70

Figure 5-9 New aggregate

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

   a. In the left pane of the System Manager panel, select **Volume** → **Create**.

   b. In the create Volume panel (Figure 5-10), select the Aggregate, Volume size, and Storage Type, and click **Create**.



Name: esx_boot_vol

Aggregate: esx_boot_aggr

Free space in aggregate is 239.04 GB

○ NAS (Used for CIFS or NFS access)

● SAN (Used for FC/FCoE or iSCSI access)

Total Size: 1 GB

Snapshot Reserve (%): 0

Data Space: 1 GB

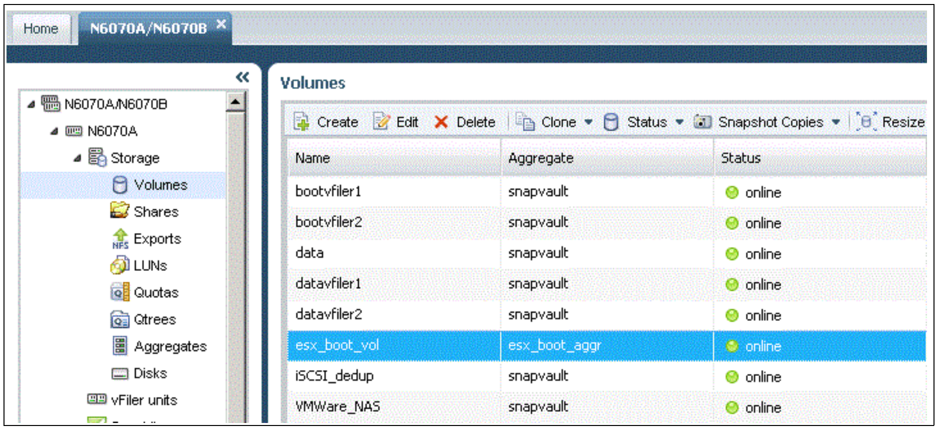
Snapshot Space: 0 Byte

□ Thin Provisioned

Allocate space as it's used, otherwise, allocate the space now. Recommended for increasing utilization when each volume is unlikely to use all of its allocated space.

Figure 5-10 Create Volume panel

c. After the volume is created, in the left pane of the System Manager panel (Figure 5-11), select **Volumes** to view the volume.



Name	Aggregate	Status
bootvfiler1	snapvault	online
bootvfiler2	snapvault	online
data	snapvault	online
datavfiler1	snapvault	online
datavfiler2	snapvault	online
esx_boot_vol	esx_boot_aggr	online
iSCSI_dedup	snapvault	online
VMWare_NAS	snapvault	online

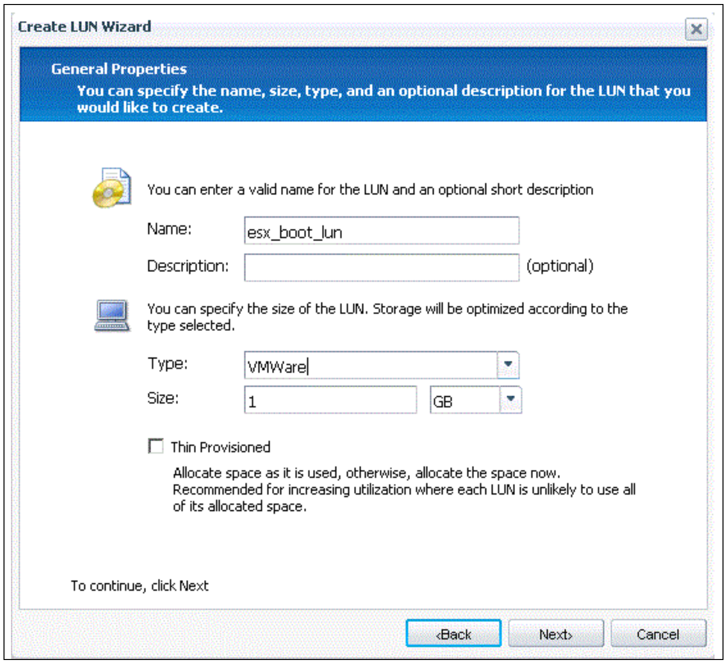
Figure 5-11 New volume

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

   a. In the left pane of the System Manager console, select **LUNs** → **Create**.

   b. Click **Next** on the Welcome panel.

   c. In the Create LUN Wizard (Figure 5-12), type the new LUN Name, select the Protocol Type and type the LUN Size. Then click **Next**.



General Properties

You can specify the name, size, type, and an optional description for the LUN that you would like to create.

You can enter a valid name for the LUN and an optional short description

Name: esx_boot_lun

Description: (optional)

You can specify the size of the LUN. Storage will be optimized according to the type selected.

Type: VMWare

Size: 1 GB

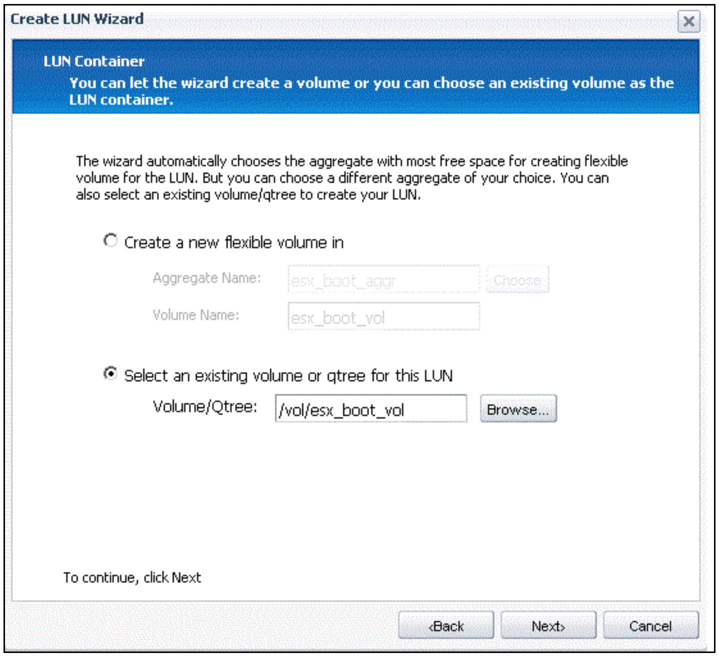
□ Thin Provisioned

Allocate space as it is used, otherwise, allocate the space now. Recommended for increasing utilization where each LUN is unlikely to use all of its allocated space.

To continue, click Next

Figure 5-12 Setting up the LUN

d. In the LUN Container panel, browse or type the Volume path created previously (Figure 5-13) and click **Next**.



Create LUN Wizard

LUN Container

You can let the wizard create a volume or you can choose an existing volume as the LUN container.

The wizard automatically chooses the aggregate with most free space for creating flexible volume for the LUN. But you can choose a different aggregate of your choice. You can also select an existing volume/qtree to create your LUN.

○ Create a new flexible volume in

Aggregate Name: esx_boot_aggr

Volume Name: esx_boot_vol

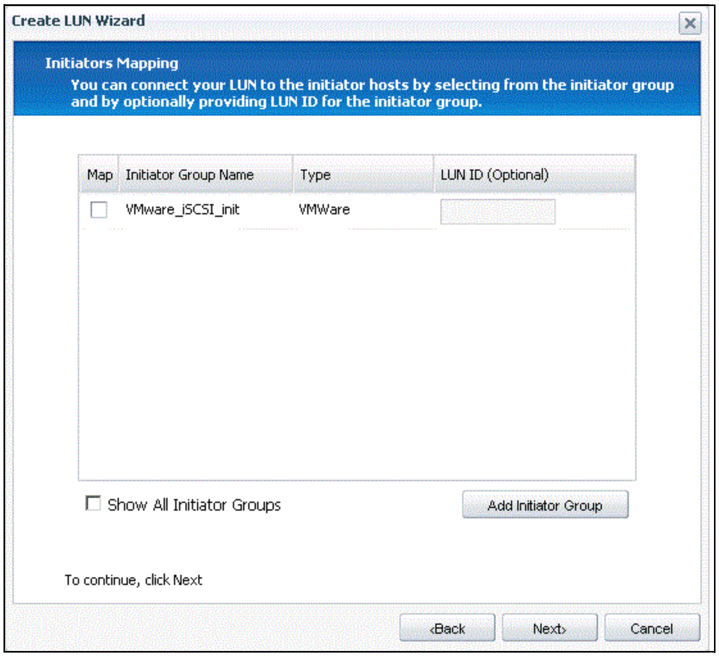
● Select an existing volume or qtree for this LUN

Volume/Qtree: /vol/esx_boot_vol

To continue, click Next

Figure 5-13 Select LUN path

e. In the next panel add an Initiator Group to map the LUN. Click **Add Initiator Group** (Figure 5-14).



Create LUN Wizard

Initiators Mapping

You can connect your LUN to the initiator hosts by selecting from the initiator group and by optionally providing LUN ID for the initiator group.

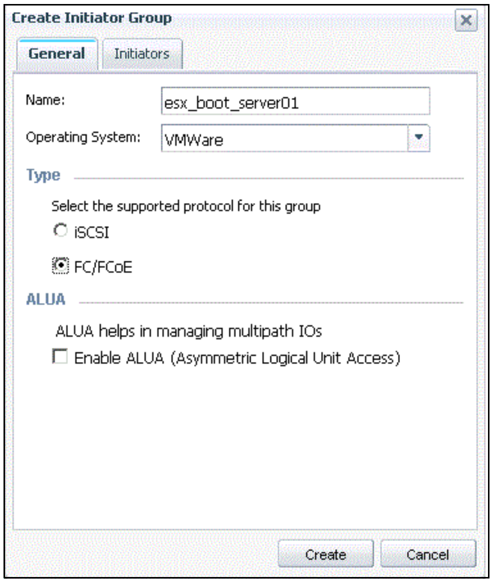
Map	Initiator Group Name	Type	LUN ID (Optional)
□	VMware_iSCSI_init	VMWare	

□ Show All Initiator Groups

To continue, click Next

Figure 5-14 Add Initiator Group

f. In the Create Initiator Group panel, type the new Initiator Group Name, select the Operating System and Protocol Type as shown in Figure 5-15.



Name: esx_boot_server01

Operating System: VMWare

Select the supported protocol for this group

○ iSCSI

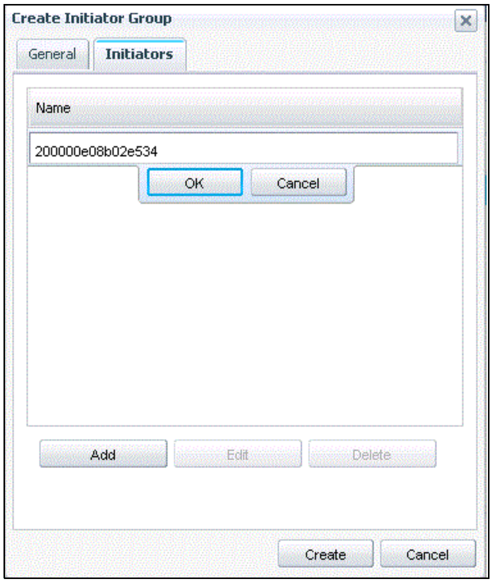
● FC/FCoE

ALUA helps in managing multipath IOs

□ Enable ALUA (Asymmetric Logical Unit Access)

Figure 5-15 Create initiator panel

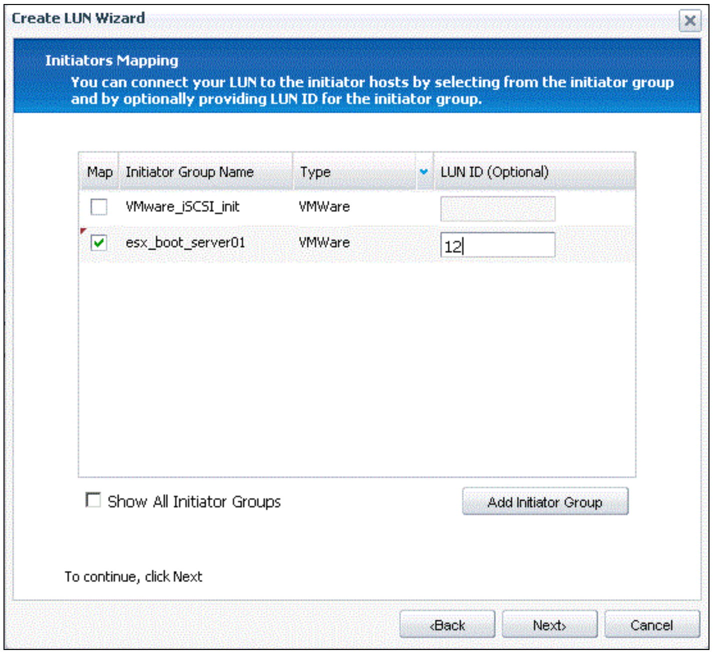
g. Still on the Create Initiator Group panel, click the **Initiators** tab, then click **Add**. In this panel, type the WWPNs or the iSCSI information for the server adapter (Figure 5-16) based on which protocol you selected on the previous step. Click **OK** and **Create**.



200000e08b02e534

Figure 5-16 Initiator adapter information

h. Back to the Initiator Mapping panel, select the initiator created and type a LUN ID (Figure 5-17) and click **Next**.



Initiators Mapping

You can connect your LUN to the initiator hosts by selecting from the initiator group and by optionally providing LUN ID for the initiator group.

Map	Initiator Group Name	Type	LUN ID (Optional)
☐	VMware_iSCSI_init	VMWare	
☑	esx_boot_server01	VMWare	12

☐ Show All Initiator Groups

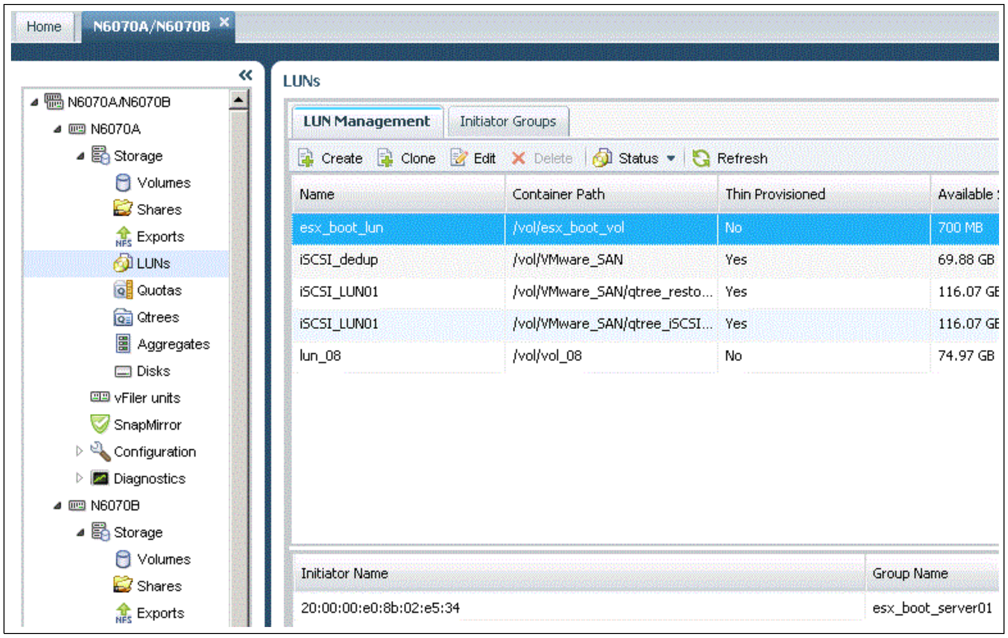
To continue, click Next

Figure 5-17 Initiator mapping panel

Tip: Type a LUN ID is not mandatory, but helps to identify the LUNs when you have many mapped to a specific server.

i. Click **Next** on the Summary Review panel to create the LUN, then click **Finish**.

j. To see the new LUN, in the left pane of the System Manager panel (Figure 5-18), select **LUNs**. You will be able to see that the mapping is already done also.



Name	Container Path	Thin Provisioned	Available :
esx_boot_lun	/vol/esx_boot_vol	No	700 MB
iSCSI_dedup	/vol/VMware_SAN	Yes	69.88 GB
iSCSI_LUN01	/vol/VMware_SAN/qtree_resto...	Yes	116.07 GE
iSCSI_LUN01	/vol/VMware_SAN/qtree_iSCSI...	Yes	116.07 GE
lun_08	/vol/vol_08	No	74.97 GB

Initiator Name	Group Name
20:00:00:e0:8b:02:e5:34	esx_boot_server01

Figure 5-18 New LUN without mapping

5.3.2 Zoning a LUN in the SAN switch

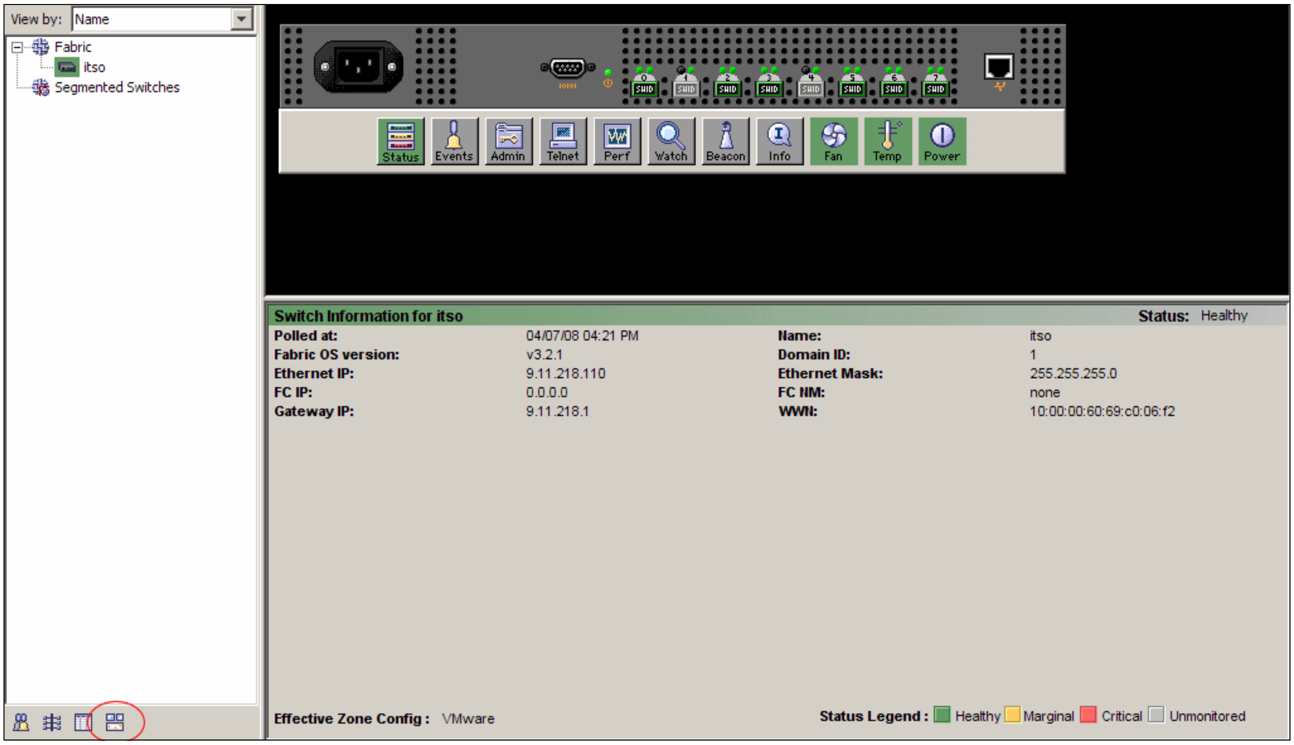
Because the connection of a bootable LUN for the VMware ESXi operation system must go through a SAN switch, you must properly zone the bootable LUN to the server’s HBA:

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 5-19).



Switch Information for itso

Status: Healthy

Polled at: 04/07/08 04:21 PM

Fabric OS version: v3.2.1

Ethernet IP: 9.11.218.110

FC IP: 0.0.0.0

Gateway IP: 9.11.218.1

Name: itso

Domain ID: 1

Ethernet Mask: 255.255.255.0

FC NM: none

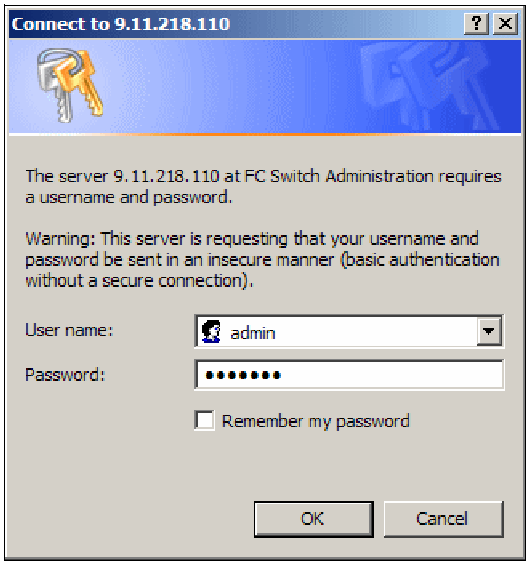
WWN: 10:00:00:60:69:c0:06:f2

Effective Zone Config : VMware

Status Legend : 🟩 Healthy 🟨 Marginal 🟥 Critical □ Unmonitored

Figure 5-19 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 5-20. Then click **OK**.



Connect to 9.11.218.110

The server 9.11.218.110 at FC Switch Administration requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

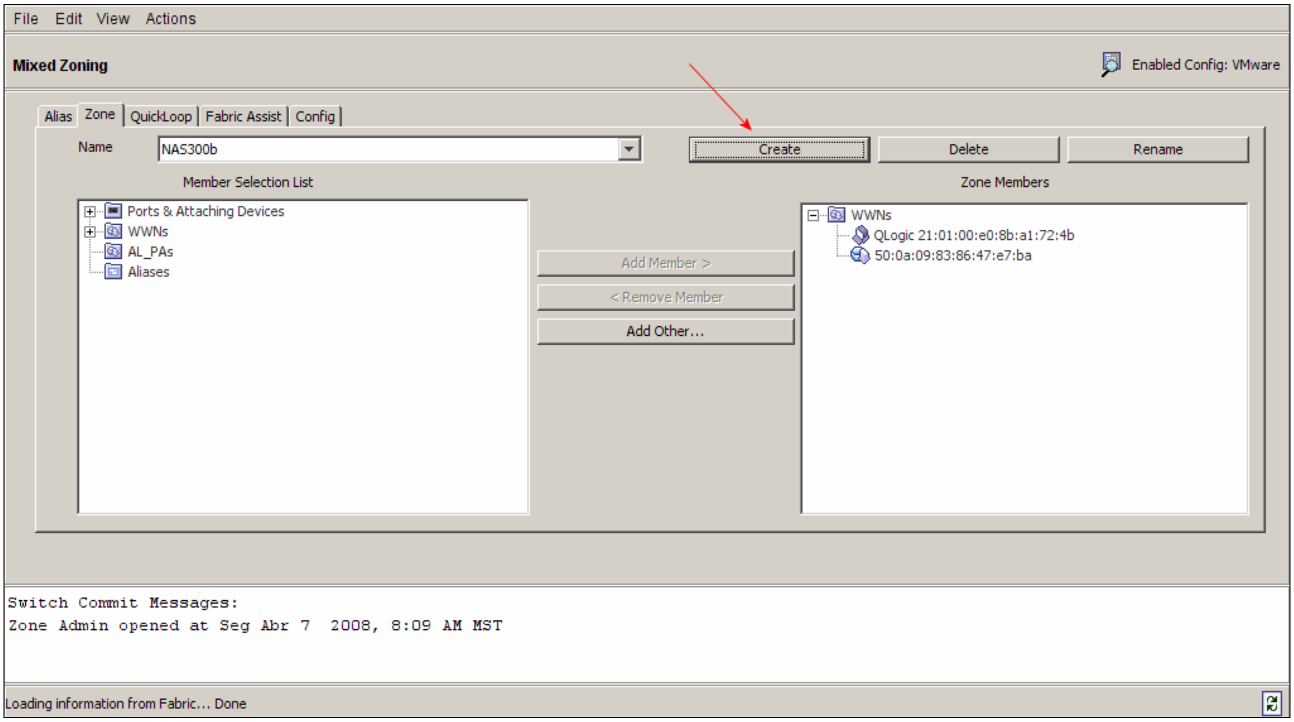
User name: admin

Password: •••••••

□ Remember my password

Figure 5-20 Signing on to access the zoning feature of the SAN switch

4. In the LUN zoning window (Figure 5-21), on the **Zone** tab, click the **Create** button to add a new zone.



Name: NAS300b

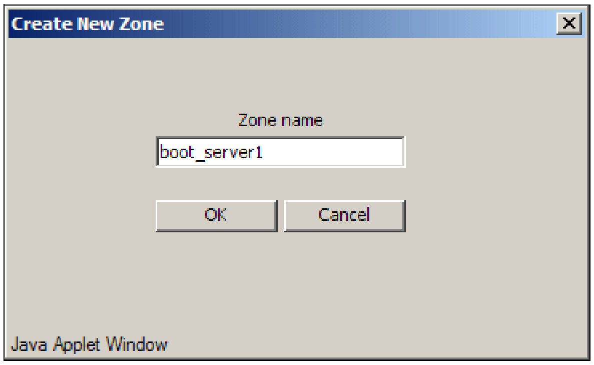
Zone Members:
- WWNs
  - QLogic 21:01:00:e0:8b:a1:72:4b
  - 50:0a:09:83:86:47:e7:ba

```
Switch Commit Messages:
Zone Admin opened at Seg Abr 7  2008, 8:09 AM MST
```

Loading information from Fabric... Done

Figure 5-21 Creating a new zone

a. In the Create New Zone window (Figure 5-22), give the new zone a name. In this example, we name it boot_server1. Then click **OK**.



Zone name: boot_server1

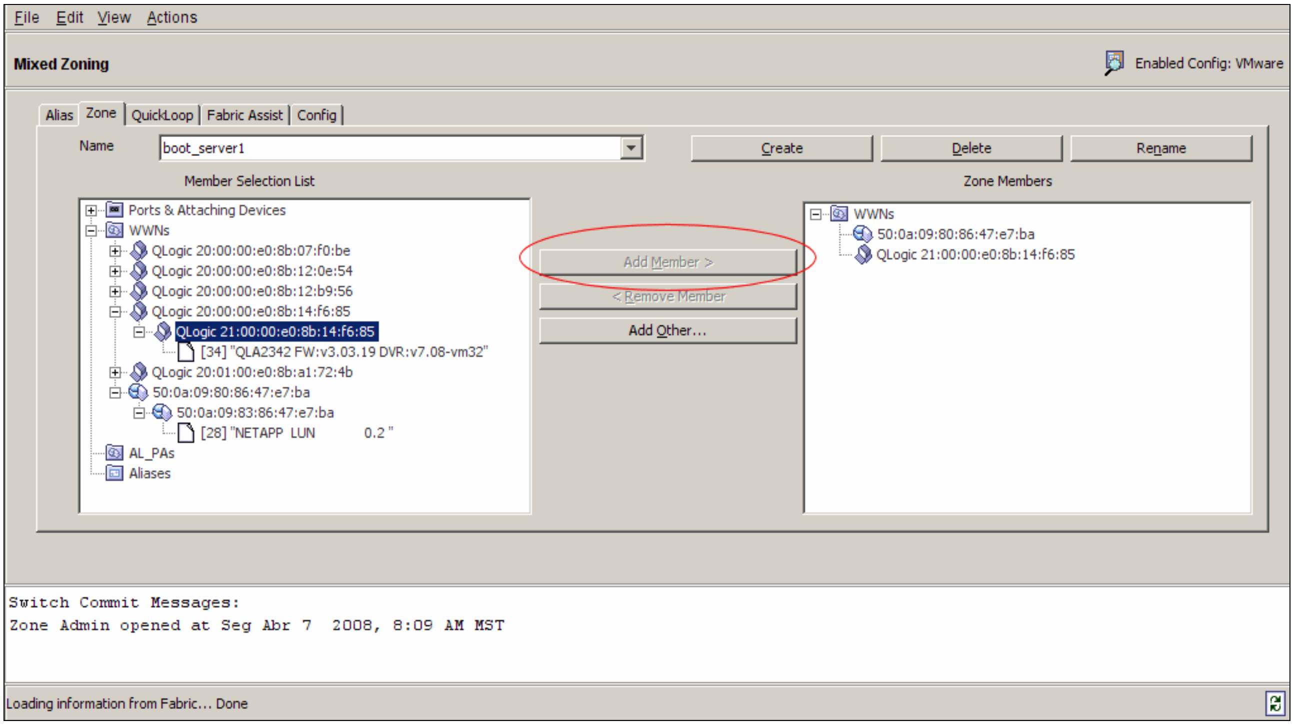
Figure 5-22 Naming the new zone

b. Assign the proper WWPNs of the storage system and the server's HBA to the new zone (Figure 5-23):

   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.



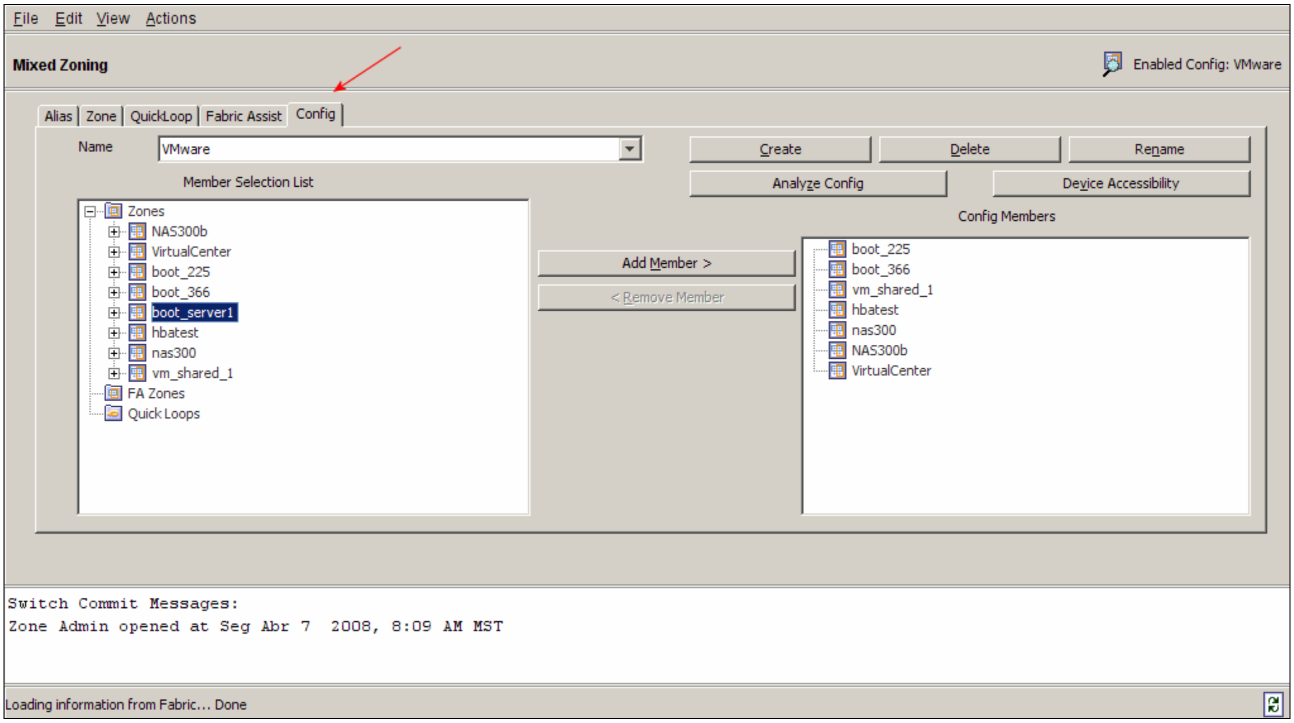
Name: boot_server1

```
Switch Commit Messages:
Zone Admin opened at Seg Abr 7  2008, 8:09 AM MST
```

Loading information from Fabric... Done

Figure 5-23 Assigning the WWPNs of the storage system and server HBA to the zone

5. Click the **Config** tab (Figure 5-24) 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.



Mixed Zoning

Enabled Config: VMware

Name: VMware

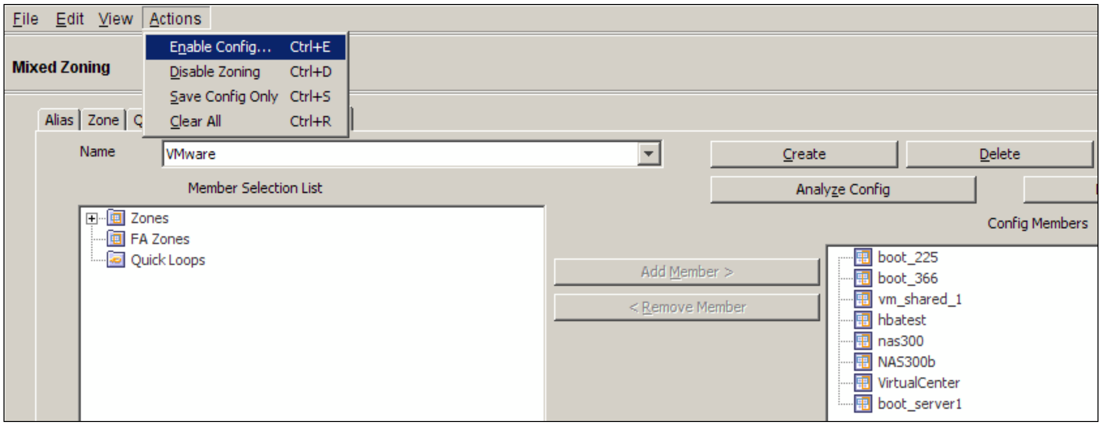
```
Switch Commit Messages:
Zone Admin opened at Seg Abr 7  2008, 8:09 AM MST
```

Loading information from Fabric... Done

Figure 5-24 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 5-25.

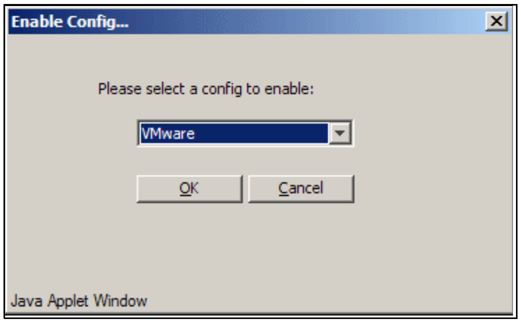


Mixed Zoning

Name: VMware

Figure 5-25 Enabling the SAN switch configuration

b. In the Enable Config window (Figure 5-26), select the configuration to enable. In this example, we select **VMware** configuration. Click **OK**.

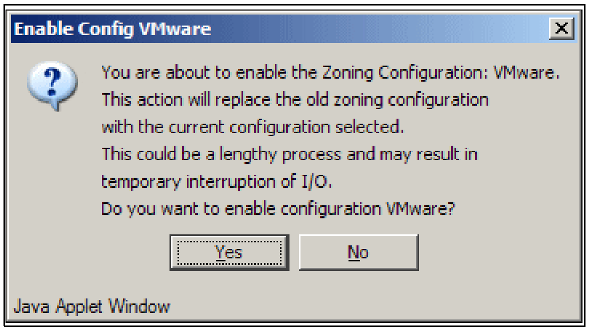


Please select a config to enable:

VMware

Figure 5-26 LUN zoning - enable configuration selection

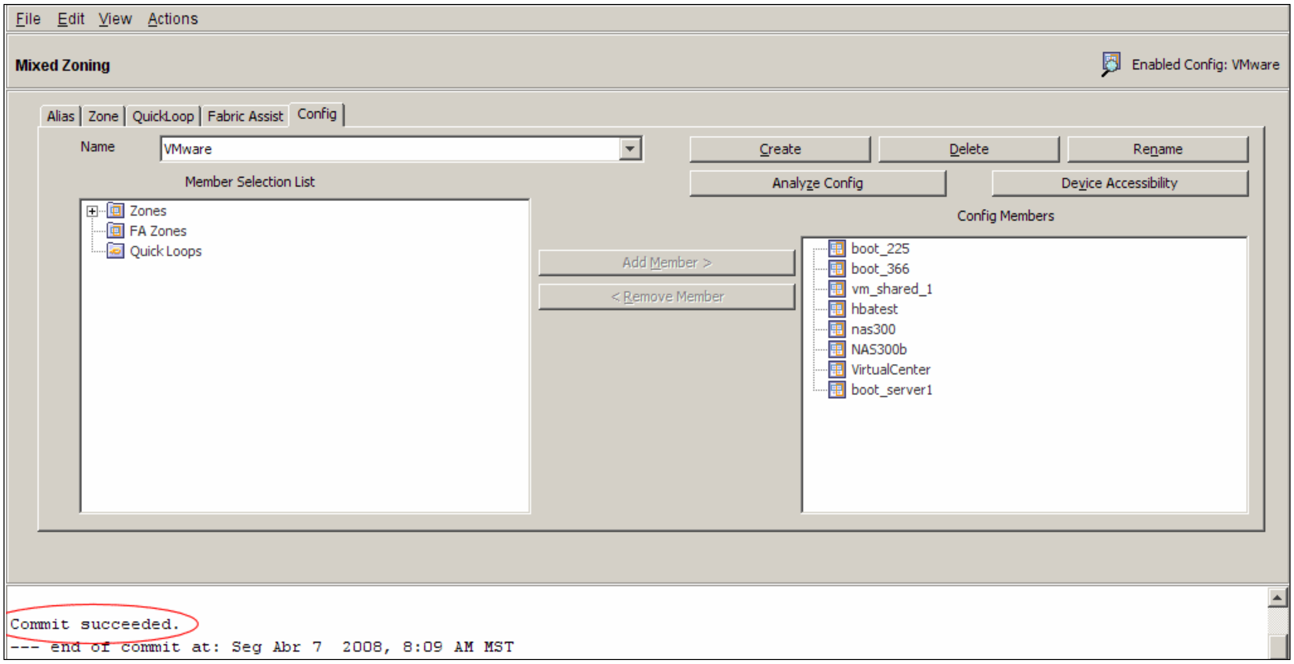
c. In the Enable Config VMware message box (Figure 5-27), click **Yes**.



You are about to enable the Zoning Configuration: VMware.
This action will replace the old zoning configuration
with the current configuration selected.
This could be a lengthy process and may result in
temporary interruption of I/O.
Do you want to enable configuration VMware?

Figure 5-27 Replacing the SAN switch configuration

Figure 5-28 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.



Enabled Config: VMware

Name: VMware

Config Members:
- boot_225
- boot_366
- vm_shared_1
- hbatest
- nas300
- NAS300b
- VirtualCenter
- boot_server1

```
Commit succeeded.
--- end of commit at: Seg Abr 7  2008, 8:09 AM MST
```

Figure 5-28 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, you can configure the HBA device of the server as a bootable device.

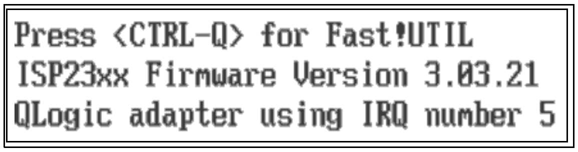
EMULEX HBAs: This example shows how to configure a QLogic HBA as a boot device. For EMULEX HBAs, see the EMULEX documentation at the following website:

`https://community.emc.com/docs/DOC-10015`

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 5-29).



```
Press <CTRL-Q> for Fast!UTIL
ISP23xx Firmware Version 3.03.21
QLogic adapter using IRQ number 5
```

Figure 5-29 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 5-30), use the arrows keys to highlight the **Configuration Settings** option and press Enter.

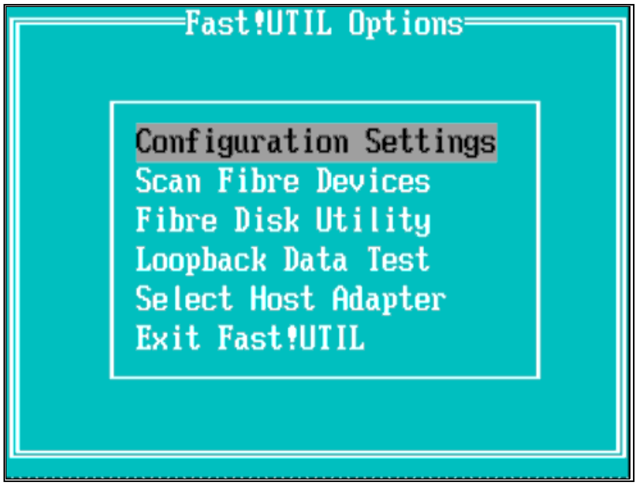
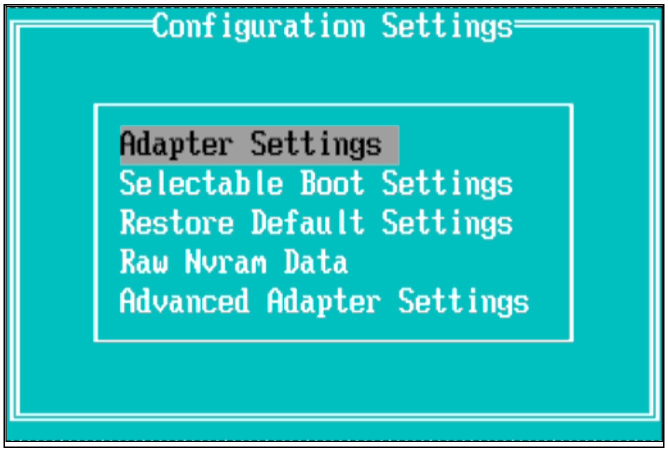


Figure 5-30 Selecting the Configuration Settings option

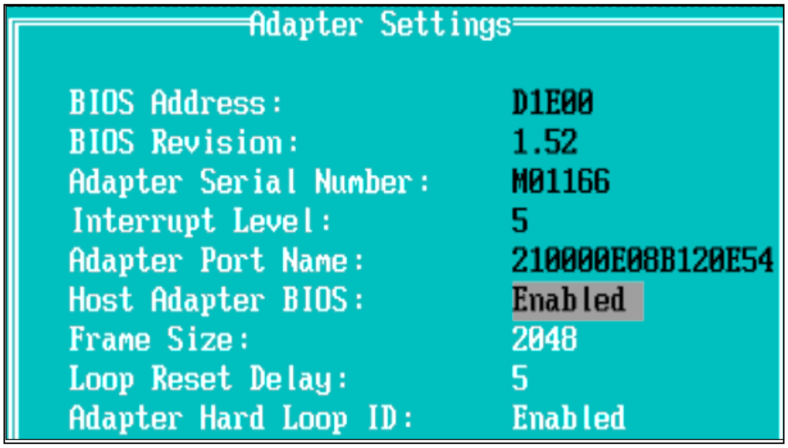
4. In the Configuration Settings panel (Figure 5-31), select **Adapter Settings** and press Enter.



```
Configuration Settings

Adapter Settings
Selectable Boot Settings
Restore Default Settings
Raw Nvram Data
Advanced Adapter Settings
```

Figure 5-31 Selecting the Adapter Settings option

5. In the Adapter Settings panel (Figure 5-32), 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.



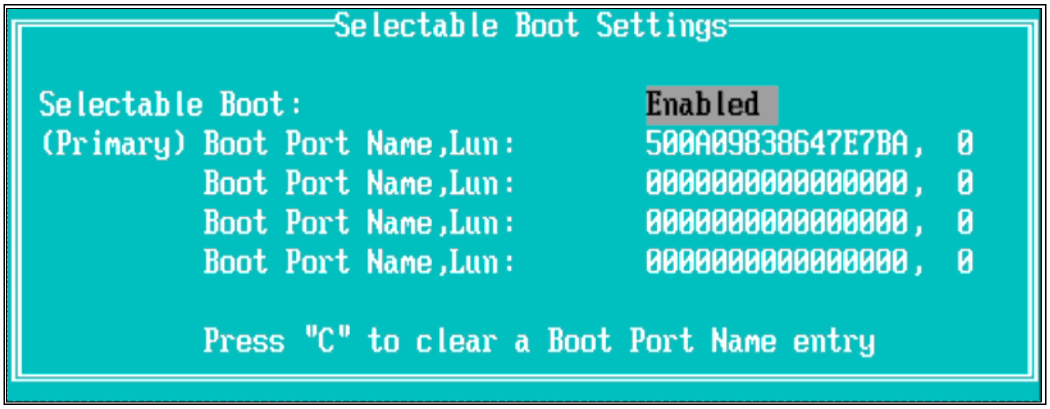
```
Adapter Settings

BIOS Address:               D1E00
BIOS Revision:              1.52
Adapter Serial Number:      M01166
Interrupt Level:            5
Adapter Port Name:          210000E08B120E54
Host Adapter BIOS:          Enabled
Frame Size:                 2048
Loop Reset Delay:           5
Adapter Hard Loop ID:       Enabled
```

Figure 5-32 Enabling Host Adapter BIOS

6. In the Configuration Settings panel as shown before (Figure 5-31), select the **Selectable boot settings** option and press Enter.

7. In the Selectable Boot Settings panel (Figure 5-33), 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.



```
                    Selectable Boot Settings

Selectable Boot:                          Enabled
(Primary) Boot Port Name,Lun:             500A09838647E7BA,  0
          Boot Port Name,Lun:             0000000000000000,  0
          Boot Port Name,Lun:             0000000000000000,  0
          Boot Port Name,Lun:             0000000000000000,  0

          Press "C" to clear a Boot Port Name entry
```

Figure 5-33 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 5-34).

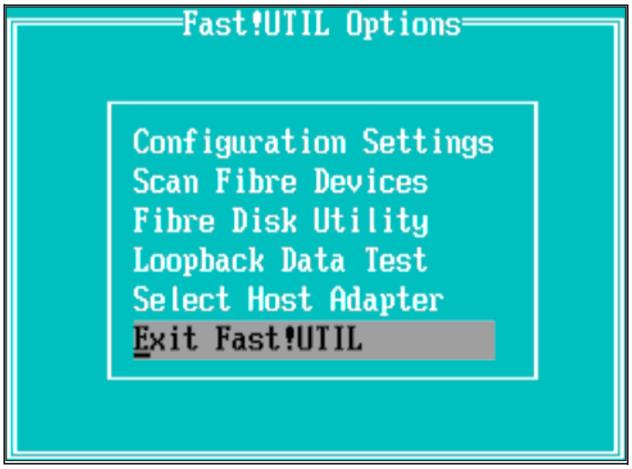


Figure 5-34 HBA setup

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 5-35), use the arrow keys to highlight **Start Options**. Press Enter.

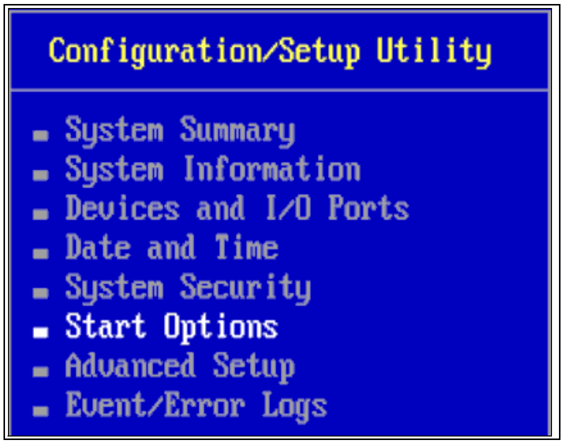


Figure 5-35 Selecting Start Options

3. In the Start Options panel (Figure 5-36), select **Startup Sequence Options** and press Enter.

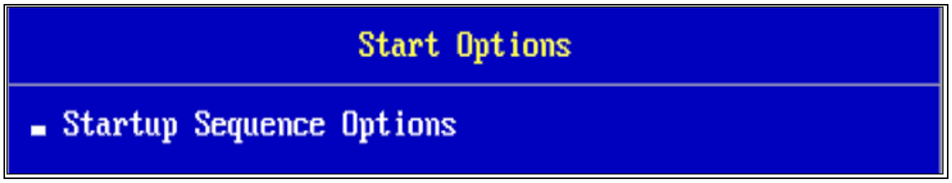
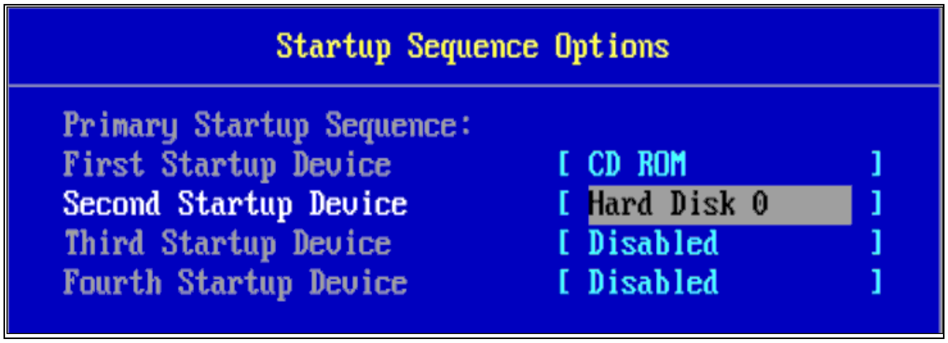


Figure 5-36 Selecting Startup Sequence Options

4. In the Startup Sequence Options panel (Figure 5-37), for First Startup Device, type `CD ROM`, and for Second Startup Device, type `Hard Disk 0`. Press Esc to return.



```
Startup Sequence Options

Primary Startup Sequence:
First Startup Device          [ CD ROM       ]
Second Startup Device         [ Hard Disk 0  ]
Third Startup Device          [ Disabled     ]
Fourth Startup Device         [ Disabled     ]
```

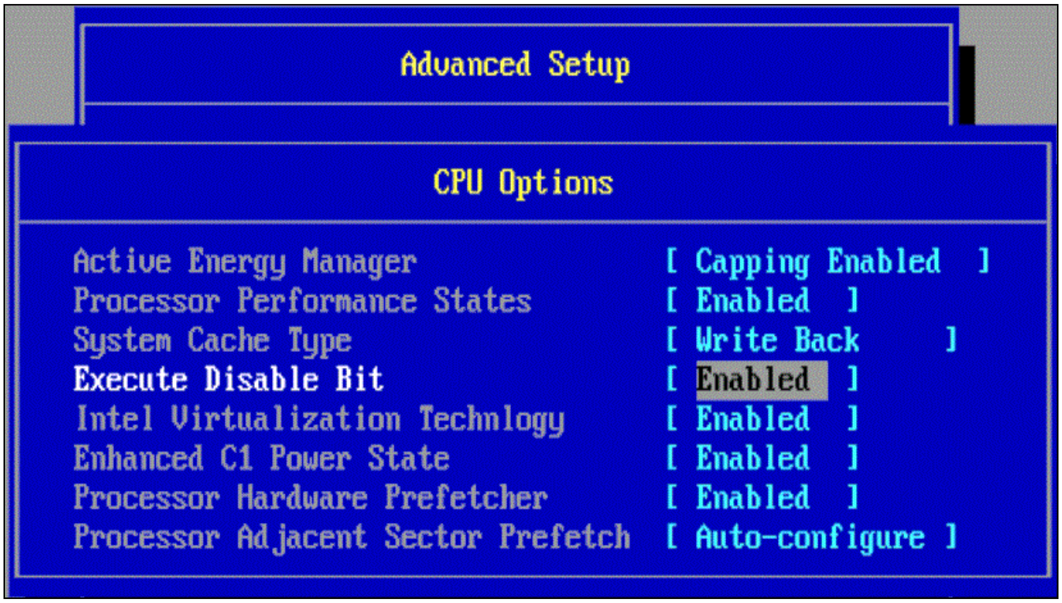
Figure 5-37 Specifying the first and second startup devices

Executing the Disable Bit feature

Two new requirements must be addressed on the server BIOS:

- ESXi 5.1 supports only LAHF and SAHF CPU instructions.
- ESXi 5.1 requires the NX/XD bit to be enabled for the CPU in the BIOS.

It means that the following feature also needs to be enabled as shown in Figure 5-38.

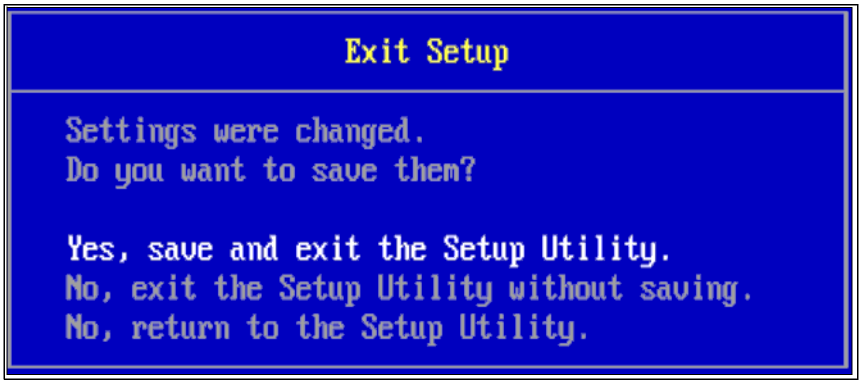


```
                    Advanced Setup

                     CPU Options

  Active Energy Manager             [ Capping Enabled  ]
  Processor Performance States      [ Enabled  ]
  System Cache Type                 [ Write Back     ]
  Execute Disable Bit               [ Enabled  ]
  Intel Virtualization Technlogy    [ Enabled  ]
  Enhanced C1 Power State           [ Enabled  ]
  Processor Hardware Prefetcher     [ Enabled  ]
  Processor Adjacent Sector Prefetch [ Auto-configure ]
```

Figure 5-38 Enable Execute Disable Bit feature

To enable this feature, follow these steps:

1. In the Exit Setup window, as shown in Figure 5-39, select **Yes, save and exit the Setup Utility**.



```
                 Exit Setup

  Settings were changed.
  Do you want to save them?

  Yes, save and exit the Setup Utility.
  No, exit the Setup Utility without saving.
  No, return to the Setup Utility.
```

Figure 5-39 Saving the changes and exiting the Setup Utility

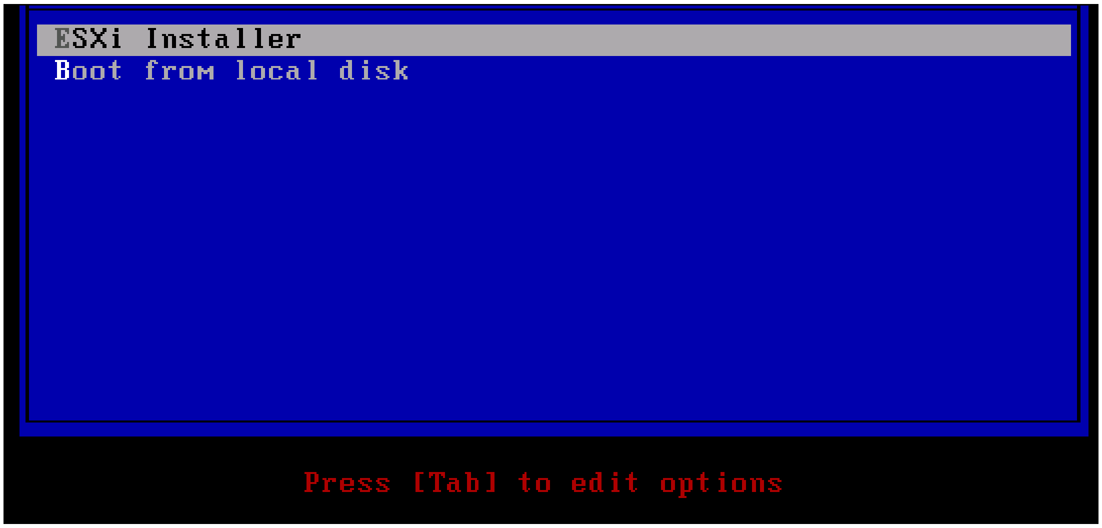
2. Reboot the server.

The server and LUN are ready for the ESXi 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 shown in Figure 5-40, choose either the graphical (GUI) or text interface. Press Enter to choose the GUI.

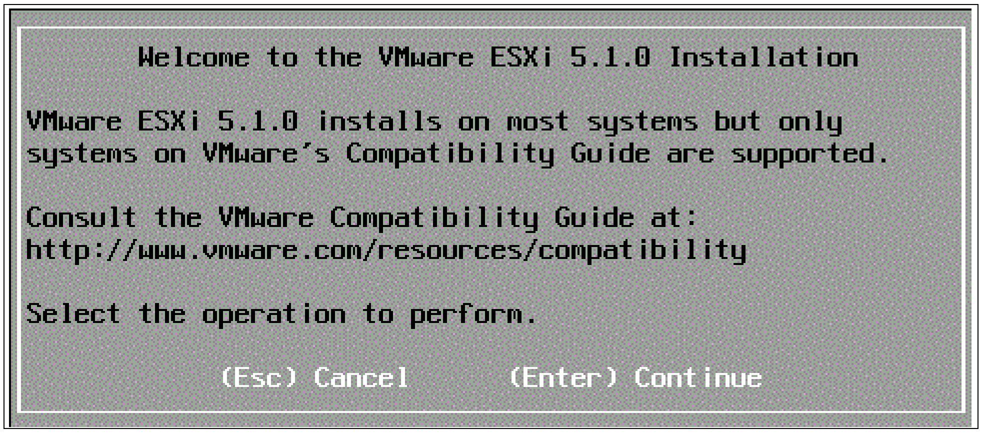


Press [Tab] to edit options

Figure 5-40 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 5-41, click **Next**.



Welcome to the VMware ESXi 5.1.0 Installation

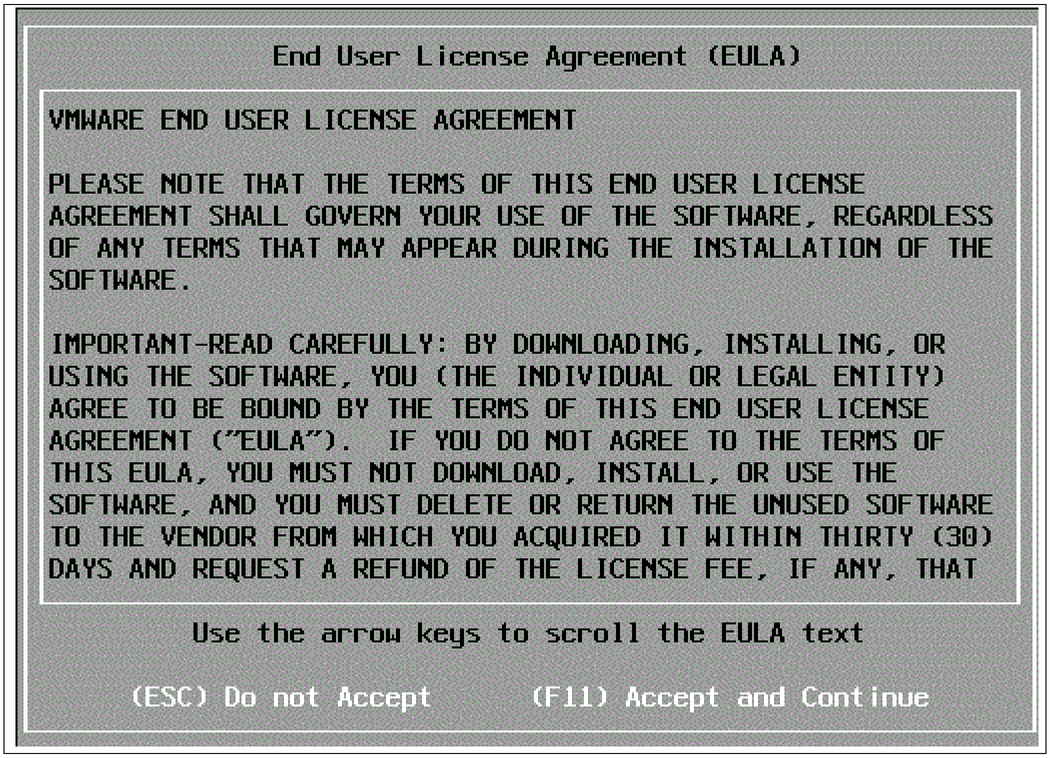
VMware ESXi 5.1.0 installs on most systems but only systems on VMware's Compatibility Guide are supported.

Consult the VMware Compatibility Guide at:
http://www.vmware.com/resources/compatibility

Select the operation to perform.

Figure 5-41 ESXi 5.1 Welcome window

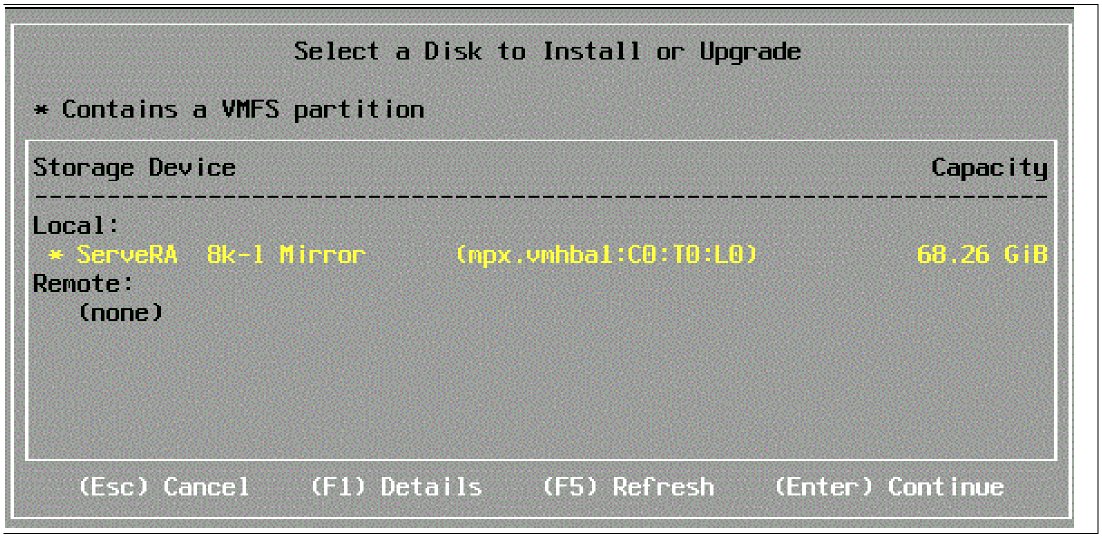
4. In the license agreement panel, in Figure 5-42, read the license text. If you agree with the terms, press F11 to proceed with the installation.



```
                End User License Agreement (EULA)

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE
AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS
OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE
SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR
USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY)
AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE
AGREEMENT ("EULA").  IF YOU DO NOT AGREE TO THE TERMS OF
THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE
SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE
TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30)
DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT

             Use the arrow keys to scroll the EULA text

        (ESC) Do not Accept       (F11) Accept and Continue
```

Figure 5-42   License agreement panel

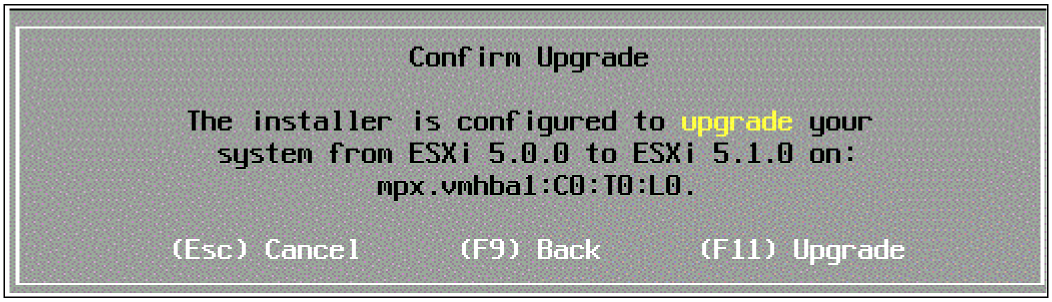
5. In the next step, shown in Figure 5-43, VMWare lists the physical disks found during its scanning. Those disks include local ones and LUNs provided to be used by the SAN boot systems panel (choose how you want to set up the initial system partition).



```
                 Select a Disk to Install or Upgrade

* Contains a VMFS partition

Storage Device                                               Capacity
----------------------------------------------------------------------
Local:
 * ServeRA  8k-1 Mirror     (mpx.vmhba1:C0:T0:L0)           68.26 GiB
Remote:
   (none)

   (Esc) Cancel    (F1) Details    (F5) Refresh    (Enter) Continue
```

Figure 5-43   Selecting the disk to install ESXi 5.1

6. Because we are upgrading the ESXi from a previous installation, the next panel (Figure 5-44) shows the upgrade confirmation.

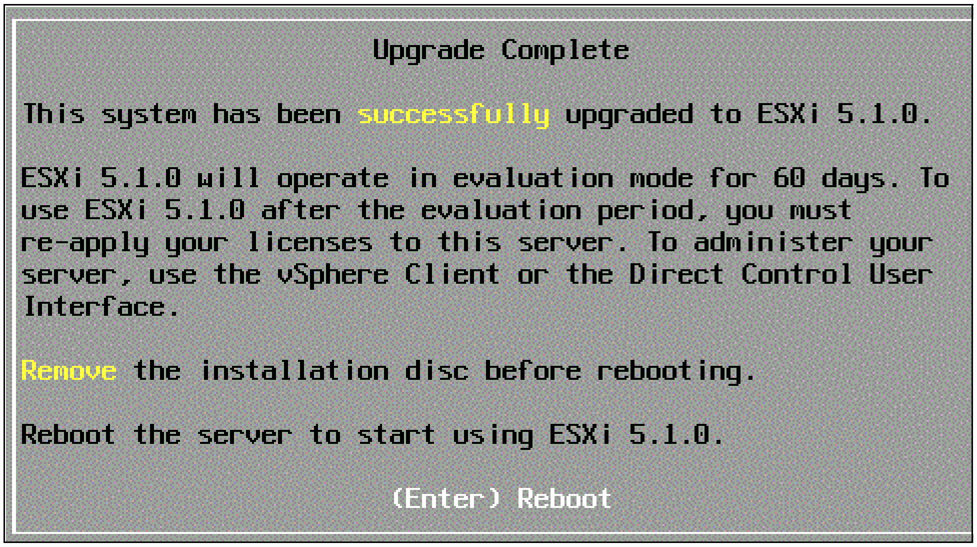


Confirm Upgrade

The installer is configured to upgrade your system from ESXi 5.0.0 to ESXi 5.1.0 on: mpx.vmhba1:C0:T0:L0.

Figure 5-44 Installer waiting the confirmation to start upgrade(F11)

7. The installation takes few minutes and finishes successfully as shown in Figure 5-45.



Upgrade Complete

This system has been successfully upgraded to ESXi 5.1.0.

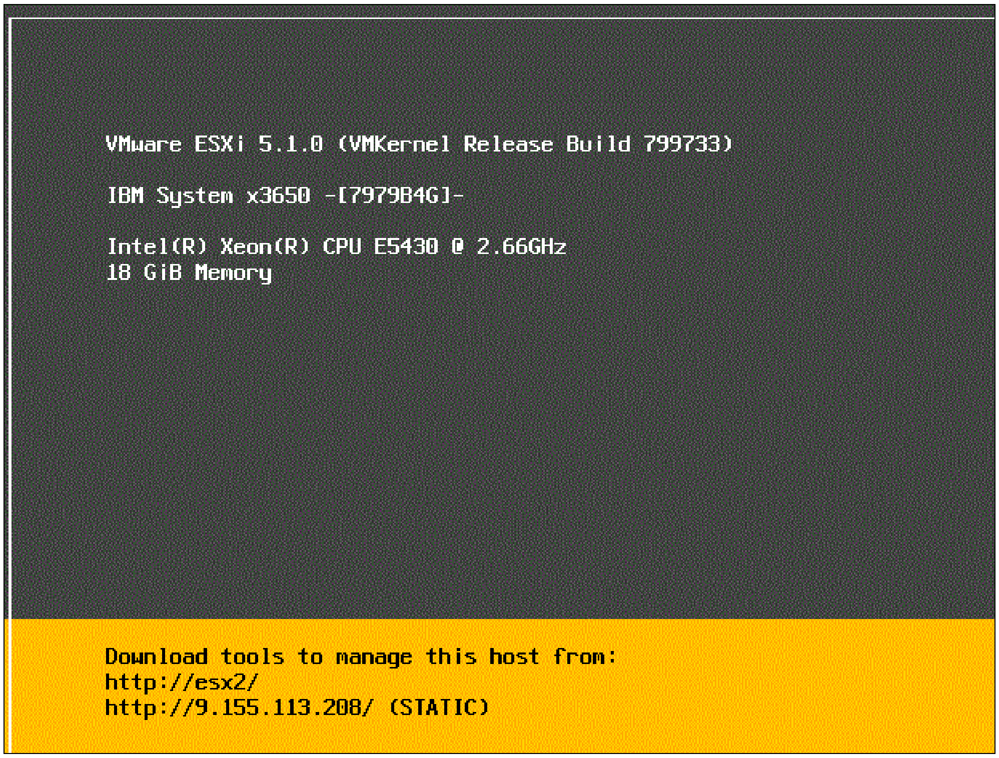
ESXi 5.1.0 will operate in evaluation mode for 60 days. To use ESXi 5.1.0 after the evaluation period, you must re-apply your licenses to this server. To administer your server, use the vSphere Client or the Direct Control User Interface.

Remove the installation disc before rebooting.

Reboot the server to start using ESXi 5.1.0.

Figure 5-45 Installation completed

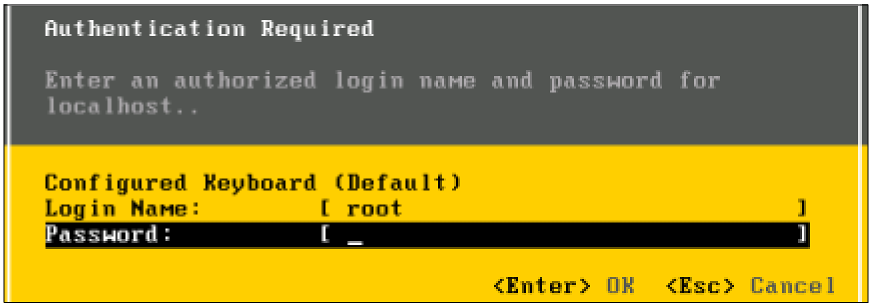
8. Remove the CD or unmount the ISO, then restart the server, and you have the following panel, as shown in Figure 5-48.



```
VMware ESXi 5.1.0 (VMKernel Release Build 799733)

IBM System x3650 -[7979B4G]-

Intel(R) Xeon(R) CPU E5430 @ 2.66GHz
18 GiB Memory

Download tools to manage this host from:
http://esx2/
http://9.155.113.208/ (STATIC)
```

Figure 5-46 Fresh installed ESXi 5.1

9. Press F2 to customize the server, then enter the root password as shown in Figure 5-47, which is empty by default, so just press Enter.



```
Authentication Required

Enter an authorized login name and password for
localhost..

Configured Keyboard (Default)
Login Name:          [ root                         ]
Password:            [ _                            ]

                              <Enter> OK   <Esc> Cancel
```

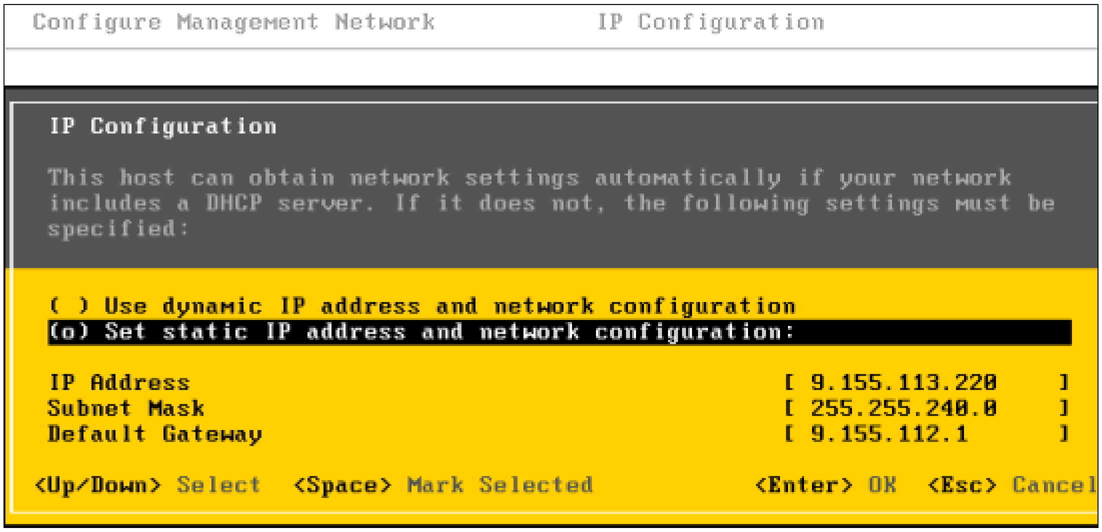
Figure 5-47 Login to the ESXi host

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.

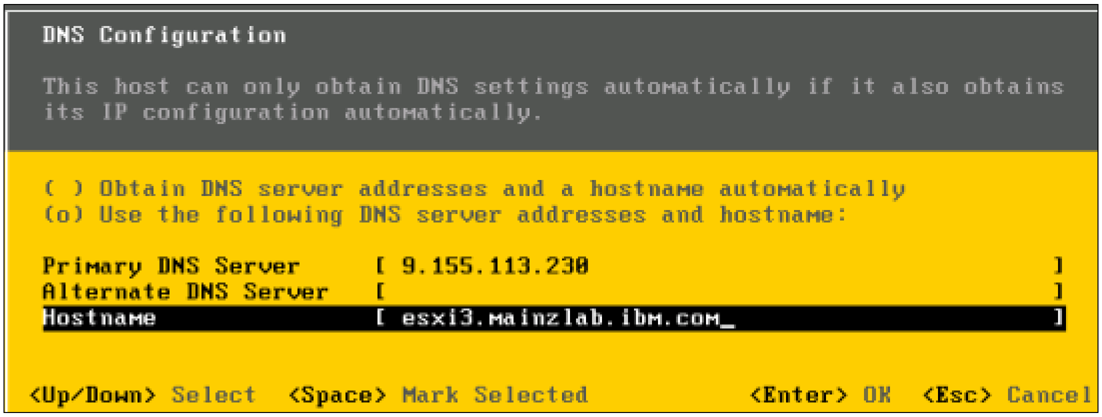
13. Then configure the host with your networking settings, as shown in Figure 5-48.



```
Configure Management Network          IP Configuration

IP Configuration

This host can obtain network settings automatically if your network
includes a DHCP server. If it does not, the following settings must be
specified:

( ) Use dynamic IP address and network configuration
(o) Set static IP address and network configuration:

IP Address                                         [ 9.155.113.220    ]
Subnet Mask                                        [ 255.255.240.0    ]
Default Gateway                                    [ 9.155.112.1      ]

<Up/Down> Select  <Space> Mark Selected          <Enter> OK  <Esc> Cancel
```

Figure 5-48 Setting network information on the host

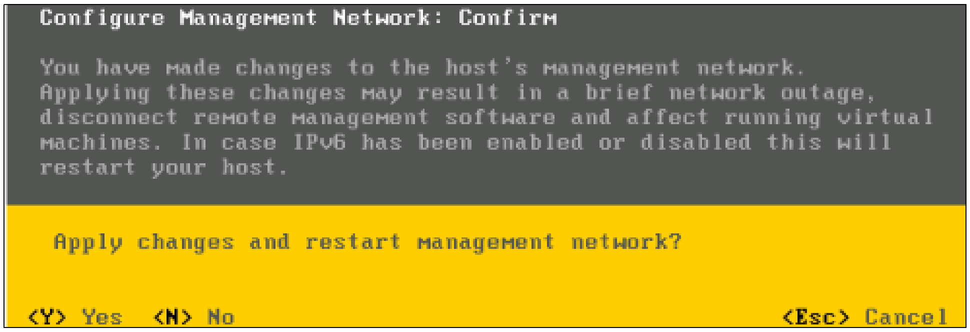
14. After setting the network, press Enter, go to **DNS configuration**, and press Enter. Type the network information and the hostname of the server, as shown in Figure 5-49. Press Enter.



```
DNS Configuration

This host can only obtain DNS settings automatically if it also obtains
its IP configuration automatically.

( ) Obtain DNS server addresses and a hostname automatically
(o) Use the following DNS server addresses and hostname:

Primary DNS Server     [ 9.155.113.230                              ]
Alternate DNS Server   [                                            ]
Hostname               [ esxi3.mainzlab.ibm.com_                    ]


<Up/Down> Select  <Space> Mark Selected          <Enter> OK  <Esc> Cancel
```

Figure 5-49 Set the DNS servers and the Hostname

15. Press Esc to leave the Configure Management Network, and on the confirmation panel, select **Y**, as shown in Figure 5-50.



```
Configure Management Network: Confirm

You have made changes to the host's management network.
Applying these changes may result in a brief network outage,
disconnect remote management software and affect running virtual
machines. In case IPv6 has been enabled or disabled this will
restart your host.

 Apply changes and restart management network?


<Y> Yes  <N> No                                    <Esc> Cancel
```

Figure 5-50 Restarting the management network to apply changes

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

17. 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 to the location where the file with the host configuration is intended to be saved.

6

Installing and configuring VMware vCenter 5.1

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

- VMware vCenter 5.1 overview
- Installing VMware vCenter 5.1
- Basic administration with VMware vCenter

© Copyright IBM Corp. 2013. All rights reserved.

6.1 VMware vCenter 5.1 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 5.1, 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 *VMware vCenter Server 5.1.0a Release Notes*, at the following website:

http://www.vmware.com/support/vsphere5/doc/vsphere-vcenter-server-510a-release-notes.html

Because our environment has less than five hosts, we use SQL 2008 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 5.1

In this book, we are using VMware vCenter version 5.1. We consider that you have a VMware registration with enough rights to perform that task and have followed the installations requisites. For more information, see the following link, *“Before You Install vCenter Server.”*

http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.install.doc%2FGUID-200B9E03-D46B-44A9-9B0E-4863D067CFFF.html

To perform the installation, follow these 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.

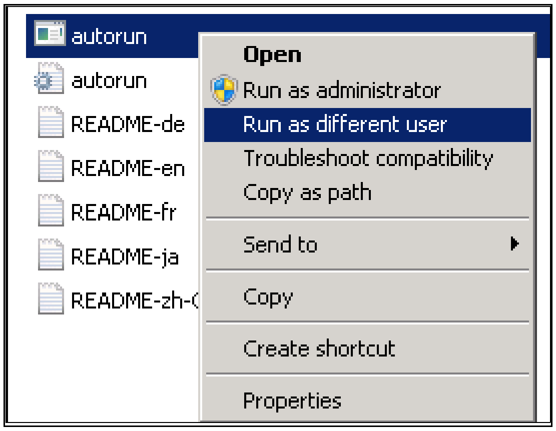


Figure 6-1 Running the installer as a different user

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

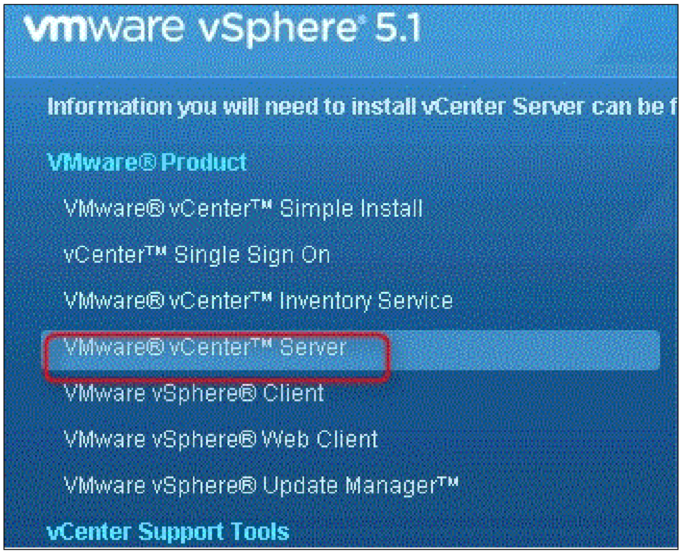
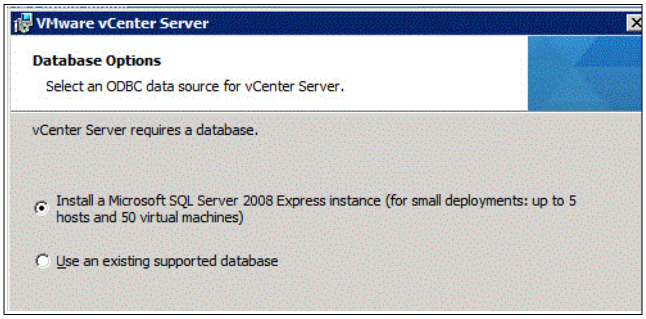

vmware vSphere 5.1
Information you will need to install vCenter Server can be f
VMware® Product
VMware® vCenter™ Simple Install
vCenter™ Single Sign On
VMware® vCenter™ Inventory Service
VMware® vCenter™ Server
VMware vSphere® Client
VMware vSphere® Web Client
VMware vSphere® Update Manager™
vCenter Support Tools

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.”* Here we use the SQL Express, as shown in Figure 6-3, but in a real environment, you would use a full bundle database. Click **Next**.



Database Options

Select an ODBC data source for vCenter Server.

vCenter Server requires a database.

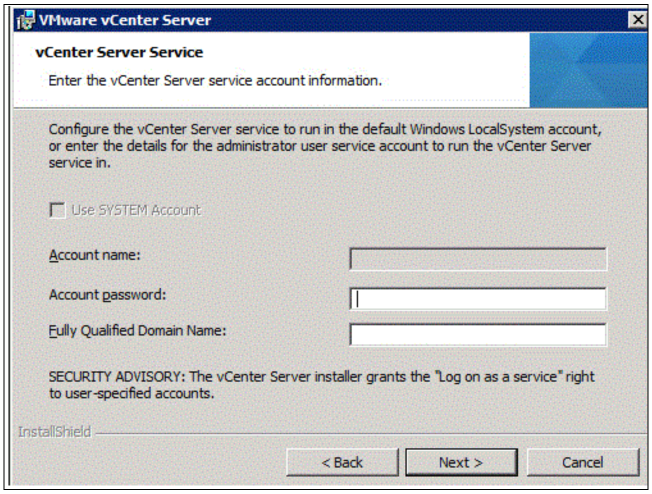
● Install a Microsoft SQL Server 2008 Express instance (for small deployments: up to 5 hosts and 50 virtual machines)

○ Use an existing supported database

Figure 6-3 Selecting the database

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

11. Because we are using Windows authentication to the SQL server (more secure than SQL authentication), you cannot enter a database username or password. Click **Next**.
12. 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**.



vCenter Server Service

Enter the vCenter Server service account information.

Configure the vCenter Server service to run in the default Windows LocalSystem account, or enter the details for the administrator user service account to run the vCenter Server service in.

□ Use SYSTEM Account

Account name:

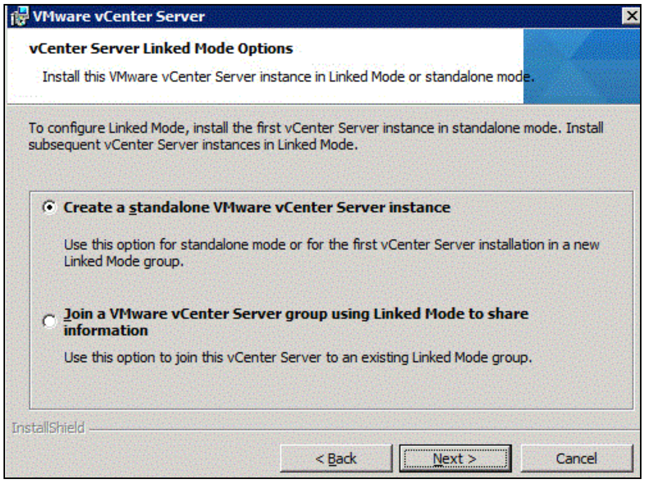
Account password:

Fully Qualified Domain Name:

SECURITY ADVISORY: The vCenter Server installer grants the "Log on as a service" right to user-specified accounts.

Figure 6-4 vCenter account during the installation

13. Because this vCenter is the first one of the structure, it must be a stand-alone instance, as shown in Figure 6-5. (If it happens to be the second or any other, you can install it as linked to the first instance, which is called a Linked Mode instance.) Click **Next**.



VMware vCenter Server

vCenter Server Linked Mode Options

Install this VMware vCenter Server instance in Linked Mode or standalone mode.

To configure Linked Mode, install the first vCenter Server instance in standalone mode. Install subsequent vCenter Server instances in Linked Mode.

● **Create a standalone VMware vCenter Server instance**

Use this option for standalone mode or for the first vCenter Server installation in a new Linked Mode group.

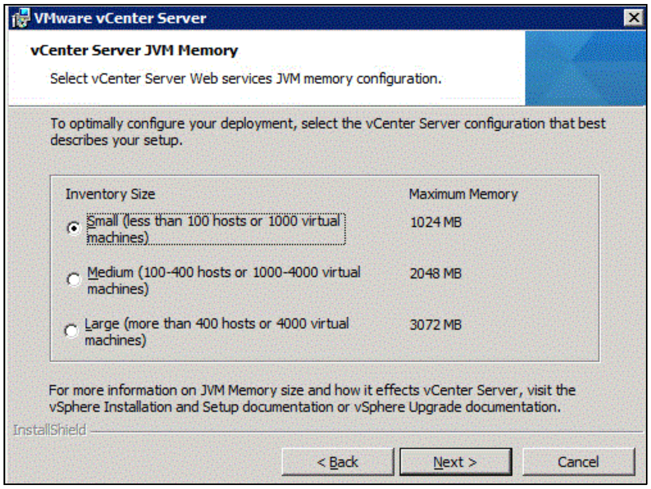
○ **Join a VMware vCenter Server group using Linked Mode to share information**

Use this option to join this vCenter Server to an existing Linked Mode group.

Figure 6-5 Creating a stand-alone instance

14. Keep the default administration ports unless they are already being used and click **Next**.

15. JVM memory is an important configuration parameter, so carefully choose the right value. If possible, select a larger value, assuming that you have adequate memory assigned to the vCenter server. See Figure 6-6.



VMware vCenter Server

vCenter Server JVM Memory

Select vCenter Server Web services JVM memory configuration.

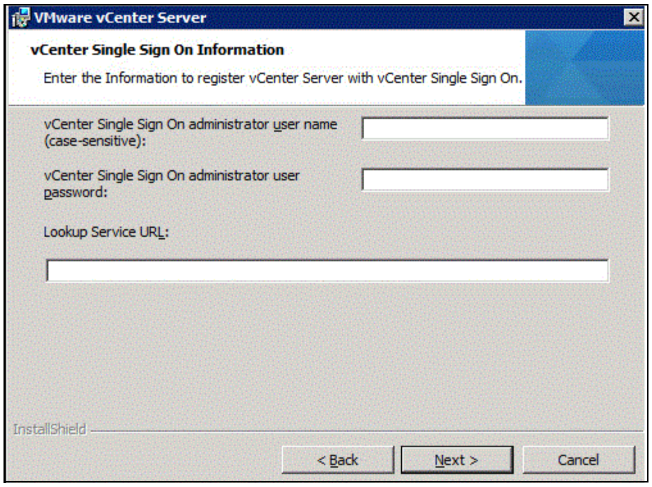
To optimally configure your deployment, select the vCenter Server configuration that best describes your setup.

Inventory Size	Maximum Memory
● Small (less than 100 hosts or 1000 virtual machines)	1024 MB
○ Medium (100-400 hosts or 1000-4000 virtual machines)	2048 MB
○ Large (more than 400 hosts or 4000 virtual machines)	3072 MB

For more information on JVM Memory size and how it effects vCenter Server, visit the vSphere Installation and Setup documentation or vSphere Upgrade documentation.

Figure 6-6 JVM memory selection panel

16. New to vSphere 5.1 is the SSO service, so you need to input the master password used during the SSO installation process as shown in Figure 6-7.


VMware vCenter Server

vCenter Single Sign On Information

Enter the Information to register vCenter Server with vCenter Single Sign On.

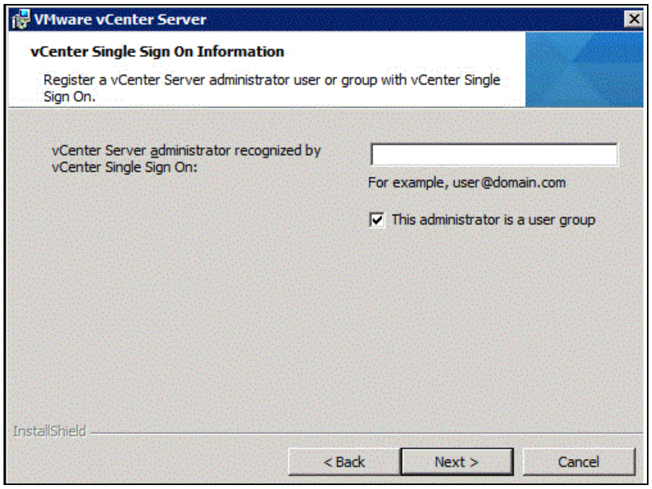
vCenter Single Sign On administrator user name (case-sensitive):

vCenter Single Sign On administrator user password:

Lookup Service URL:

Figure 6-7 vCenter SSO Information

17. At this prompt, you need to enter the group or user that will be recognized by the SSO service as the vCenter administrator, as shown in Figure 6-8.


VMware vCenter Server

vCenter Single Sign On Information

Register a vCenter Server administrator user or group with vCenter Single Sign On.

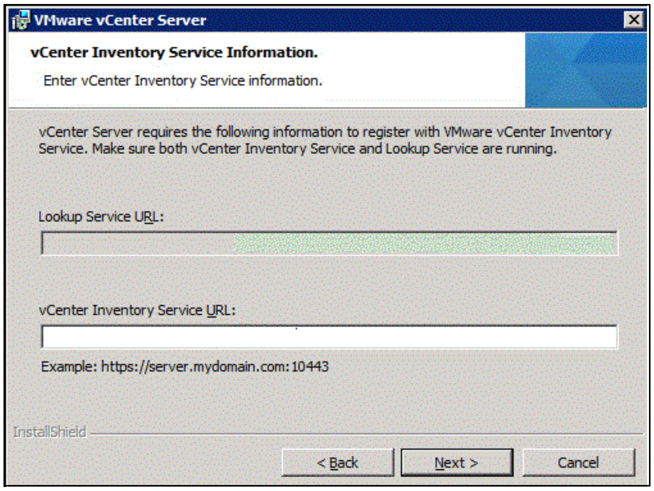
vCenter Server administrator recognized by vCenter Single Sign On:

For example, user@domain.com

☑ This administrator is a user group

Figure 6-8 SSO information

18. Next, you can see the vCenter Inventory Service URL, which needs no modifications, as shown in Figure 6-9. Click **Next**.



vCenter Inventory Service Information.

Enter vCenter Inventory Service information.

vCenter Server requires the following information to register with VMware vCenter Inventory Service. Make sure both vCenter Inventory Service and Lookup Service are running.

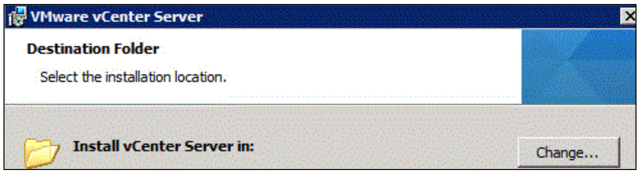
Lookup Service URL:

vCenter Inventory Service URL:

Example: https://server.mydomain.com:10443

Figure 6-9 Inventory service information

19. To facilitate administration, it is a best practice to keep the OS data separated from the application. So you need to install vCenter on another partition, as shown in Figure 6-10, and click **Next**.



Destination Folder

Select the installation location.

Install vCenter Server in:

Figure 6-10 Installing vCenter in a different partition than the OS

> **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.

20. Per a VMware you need to fix the ADAM SSL port registry type when ADWS is unable to read the ports that AD LDS is configured to use for LDAP and Secure LDAP (SSL) services. To fix this issue, check the following VMware KB:

    http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1023864

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

6.3 VMware vSphere Web Client installation

Now that vCenter Server is installed, you need to proceed to getting the vSphere Web Client installed and configured. The vSphere Web Client lets you connect to a vCenter Server system to manage an ESXi host through a browser.

The web client was first released on vCenter 5.0. It is now the primary means to manage your vSphere 5.x servers and vCenter 5.x instances (vSphere 4.x or older is not supported). In fact, nearly all new vSphere 5.1 features are only exposed through the web client. For detailed information, check this website:

http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-installation-setup-guide.pdf

6.4 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://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-host-management-guide.pdf

This section includes the following topics:

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

6.4.1 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 shown in Figure 6-11. Set its name accordingly.

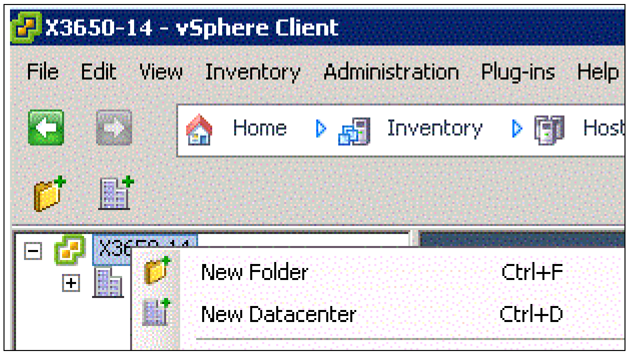


Figure 6-11 Creating a Datacenter

6.4.2 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, proceed as follows:

1. Right-click the Datacenter object, then select **New Cluster**, as shown in Figure 6-12.

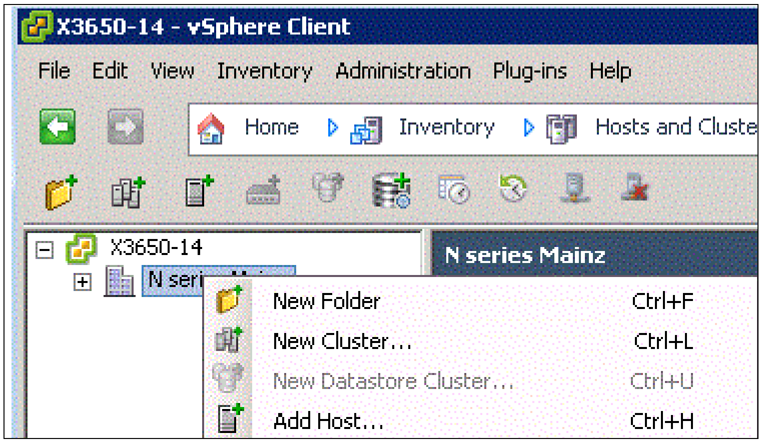
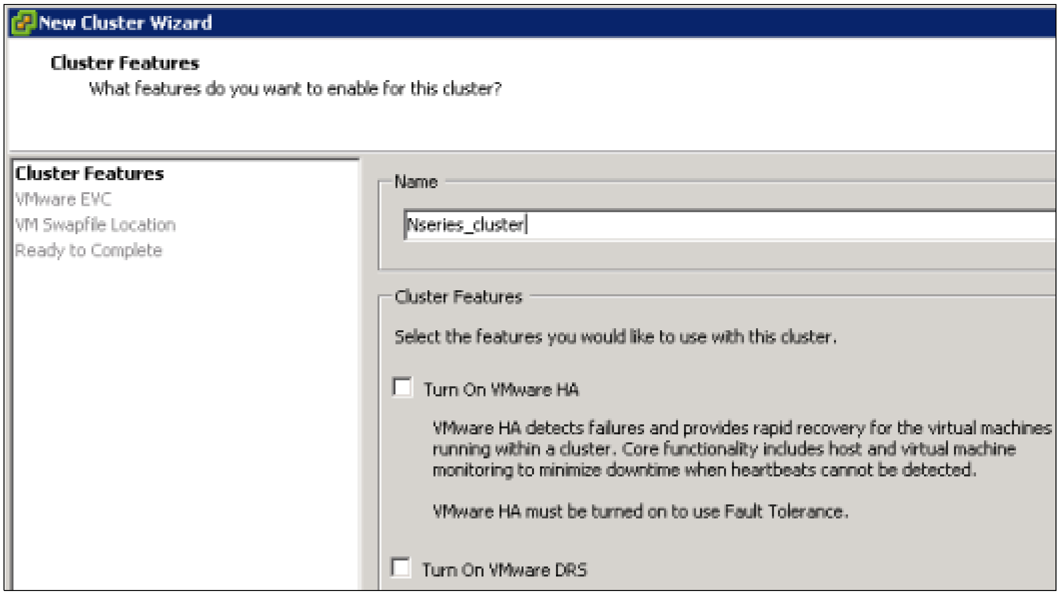


Figure 6-12 Creating a new cluster

2. On the next panel, provide a name to the cluster as shown in Figure 6-13. Select the options related to HA and DRS if you want to implement those features. Then click **Next**.



Name

Nseries_cluster

Cluster Features

Select the features you would like to use with this cluster.

□ Turn On VMware HA

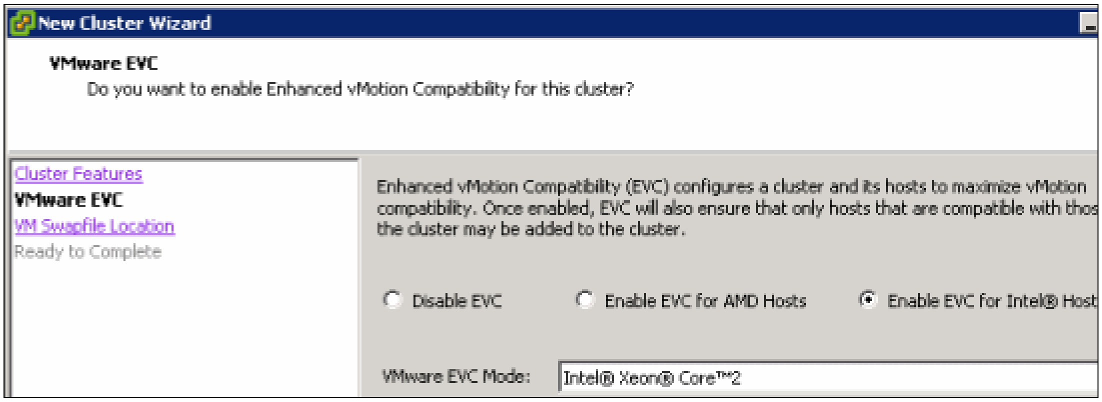
VMware HA detects failures and provides rapid recovery for the virtual machines running within a cluster. Core functionality includes host and virtual machine monitoring to minimize downtime when heartbeats cannot be detected.

VMware HA must be turned on to use Fault Tolerance.

□ Turn On VMware DRS

Figure 6-13 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 6-14. Click **Next**.



Do you want to enable Enhanced vMotion Compatibility for this cluster?

Enhanced vMotion Compatibility (EVC) configures a cluster and its hosts to maximize vMotion compatibility. Once enabled, EVC will also ensure that only hosts that are compatible with thos the cluster may be added to the cluster.

○ Disable EVC ○ Enable EVC for AMD Hosts ● Enable EVC for Intel® Host

VMware EVC Mode: Intel® Xeon® Core™2

Figure 6-14 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**.

6.4.3 Adding hosts to a cluster

Before adding a host, you must have an ESXi host already installed and set up in the network.

> **Tip:** You need to 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 6-15, right-click the cluster you want, and select **Add Host**...

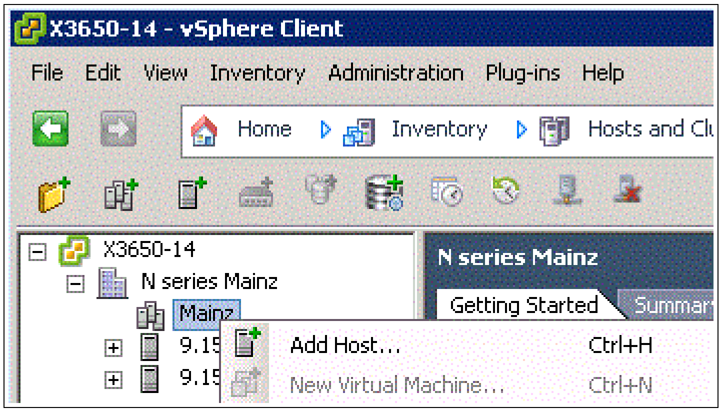
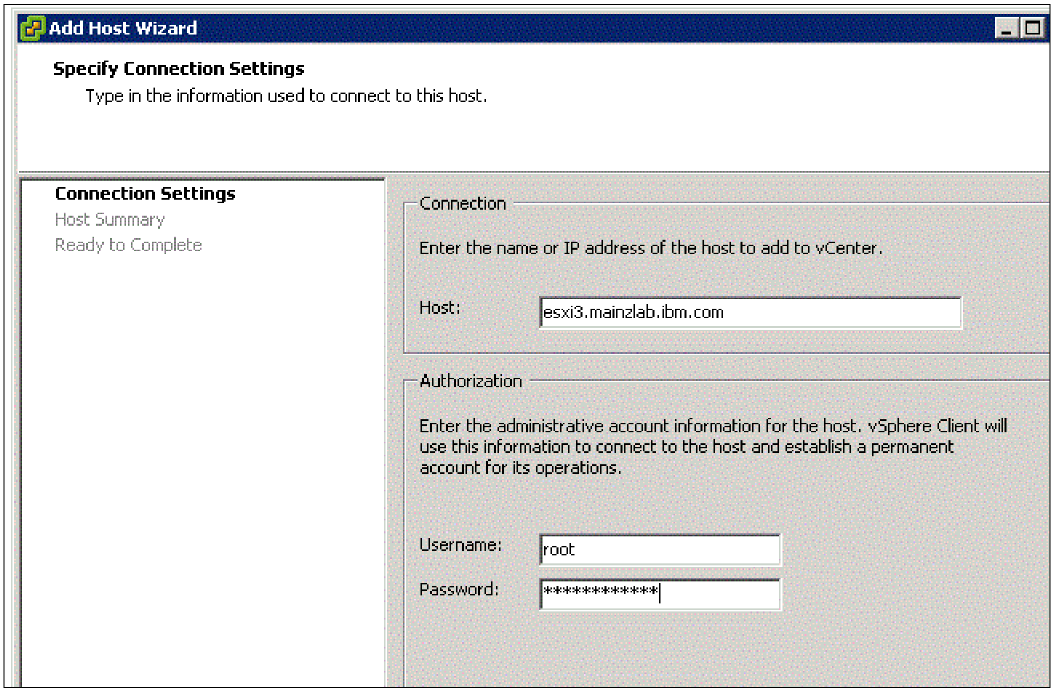


Figure 6-15 Adding a host to a cluster

2. Type the host's full qualified domain name, then root user, and its password, in the authentication box, as shown in Figure 6-16.



Specify Connection Settings

Type in the information used to connect to this host.

Connection

Enter the name or IP address of the host to add to vCenter.

Host: esxi3.mainzlab.ibm.com

Authorization

Enter the administrative account information for the host. vSphere Client will use this information to connect to the host and establish a permanent account for its operations.

Username: root

Password: *************

Figure 6-16 Adding the host name, root user, and its password

3. Accept the RSA key by clicking **OK**.
4. In the Ready to Complete panel, review the information and click **Finish**.

6.4.4 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.

To create a template, proceed as follows:

1. Just create a normal virtual machine (VM). 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 shown in Figure 6-17.

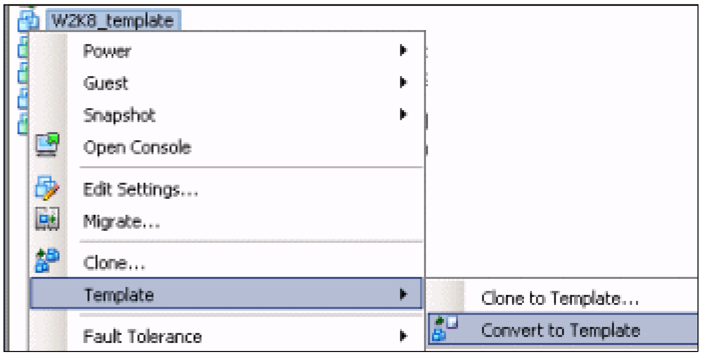


Figure 6-17 Converting a VM to a template

To see your template options, right-click one of your guests. Click **Inventory**. Select **Virtual Machines And Templates.**, as shown in Figure 6-18, and you see a panel like this one.

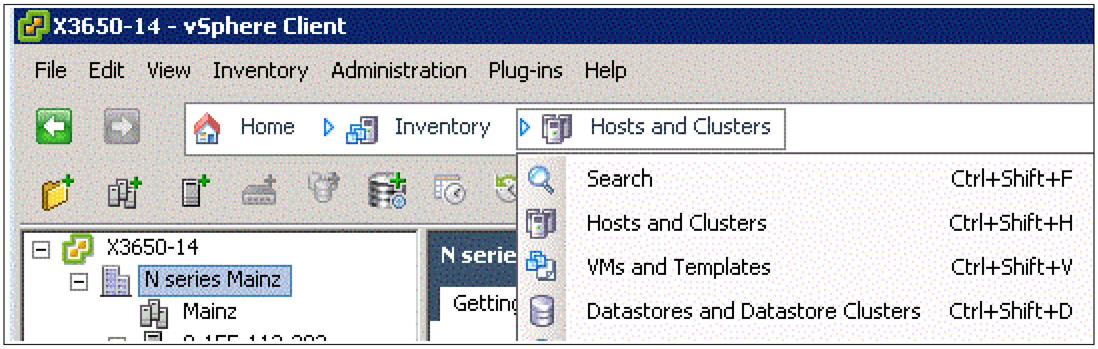


Figure 6-18 Changing view to VMs and Templates

You can see all your templates as shown in Figure 6-19.

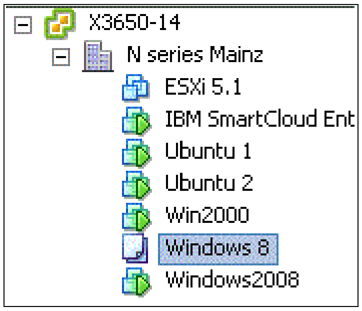


Figure 6-19 Viewing VMs and Templates

7

Presenting N series storage for VMware vSphere 5.1

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. It includes the following topics:

- Preparing N series
- Provisioning LUNs
- Creating NFS shares
- Storage growth management

© Copyright IBM Corp. 2013. All rights reserved.

7.1 Preparing N series LUNs for VMware vSphere

When provisioning LUNs for access through FC or iSCSI, they 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 (igroups).

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

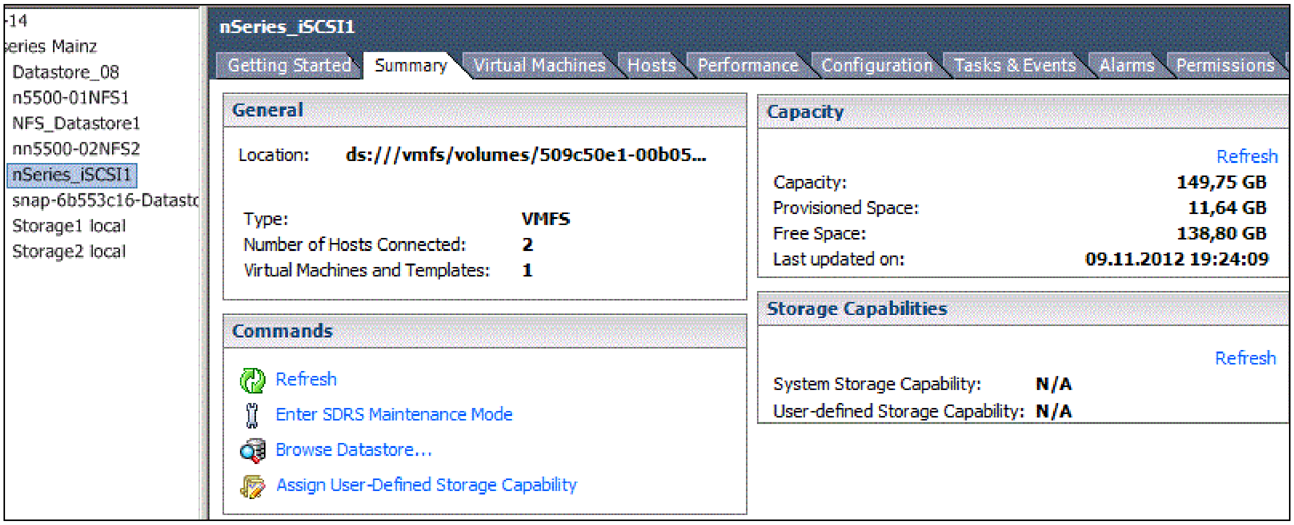
The igroup scope design depends on the virtual environment design. For instance, if you are dividing your VMWare servers into clusters that support different application tiers, you need to create an igroup for each of those clusters. That way, you ensure that all the hosts within that cluster have access to the same LUNs while avoiding the hosts from clusters to being able to see LUNs that are not relevant to them.

> **Using igroups for FC and iSCSI protocols:** Separate igroups should be created for Fibre Channel and iSCSI LUNs, even if the same membership applies to them.

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 shown in Figure 7-1.

The most common and convenient option is to create LUNs and format them as VMFS (VMware file system) for the guest operating systems. The VMFS is a multi-access and scalable file system that was developed by VMware to store the guest operating system's disk files (.vmdk), the VM‘s configuration files (.vmx and .vmxf) and BIOS information (.nvram), as well as Snapshot files when available (*0001.vmdk).

Each LUN formatted with VMFS is called a *datastore*. Figure 7-1 shows an example of using a datastore through the vCenter console.



Location: **ds:///vmfs/volumes/509c50e1-00b05...**

Type: **VMFS**
Number of Hosts Connected: **2**
Virtual Machines and Templates: **1**

Capacity: **149,75 GB**
Provisioned Space: **11,64 GB**
Free Space: **138,80 GB**
Last updated on: **09.11.2012 19:24:09**

System Storage Capability: **N/A**
User-defined Storage Capability: **N/A**

Figure 7-1 A datastore example

7.2 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 Example 7-1.

Example 7-1

```
C:\> telnet 9.155.66.113

Data ONTAP (N6070A.)
login: root
Password:
Tue Nov  6 20:06:37 CET [N6070A: telnet_0:info]: root logged in from host:
9.155.113.201
N6070A> license add <license_key>
```

Alternatively, you can use IBM N series System Manager, navigating to **Configuration** → **System Tools** → **Licenses**, and click **Add**, as shown in Figure 7-2.

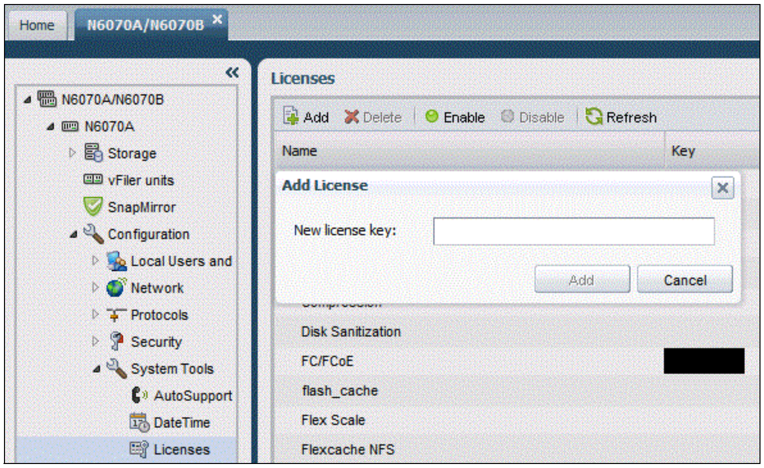


Figure 7-2 Adding licenses using GUI

7.3 Setting up thin provisioning

You can enable thin provisioning at the LUN level or volume level by using either the command line or the graphical user interface (GUI). The following sections guide you through this process using the GUI during the creation of the volumes or LUNs.

For all the next activities, you must be logged to IBM N series System Manager.

7.3.1 Enabling volume-level thin provisioning

To enable volume level thin provisioning, follow these steps:

1. In the left navigation pane, select **Storage** →**Volumes** → **Create**, as shown in Figure 7-3.

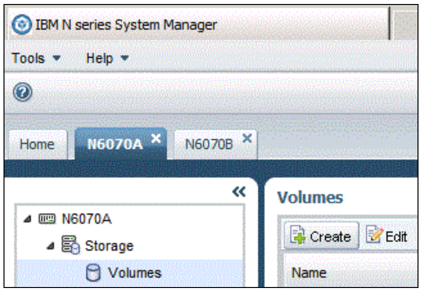
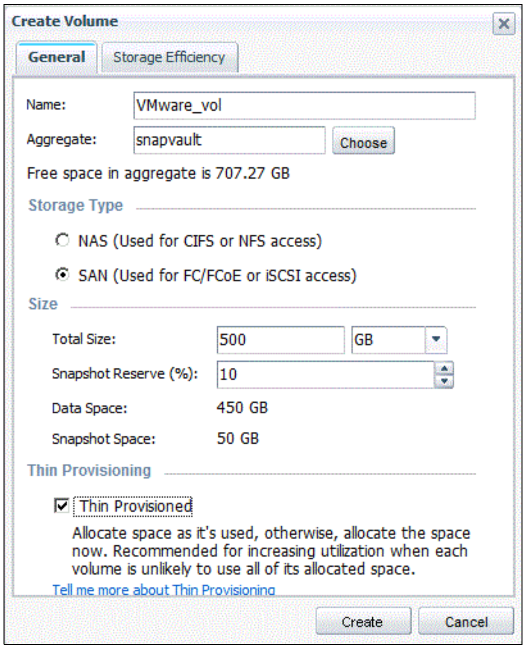


Figure 7-3 Creating a volume

2. Enter the following information on the next window (Figure 7-4):

   a. Volume name
   b. Aggregate where the volume will reside
   c. Storage type access, either NAS or SAN
   d. Total size and Snapshot reserve %
   e. Thin Provisioned check box selected



Create Volume

General | Storage Efficiency

Name: VMware_vol

Aggregate: snapvault Choose

Free space in aggregate is 707.27 GB

Storage Type

○ NAS (Used for CIFS or NFS access)

● SAN (Used for FC/FCoE or iSCSI access)

Size

Total Size: 500 GB

Snapshot Reserve (%): 10

Data Space: 450 GB

Snapshot Space: 50 GB

Thin Provisioning

☑ Thin Provisioned

Allocate space as it's used, otherwise, allocate the space now. Recommended for increasing utilization when each volume is unlikely to use all of its allocated space.

Tell me more about Thin Provisioning

Create Cancel

Figure 7-4 Adding volume information

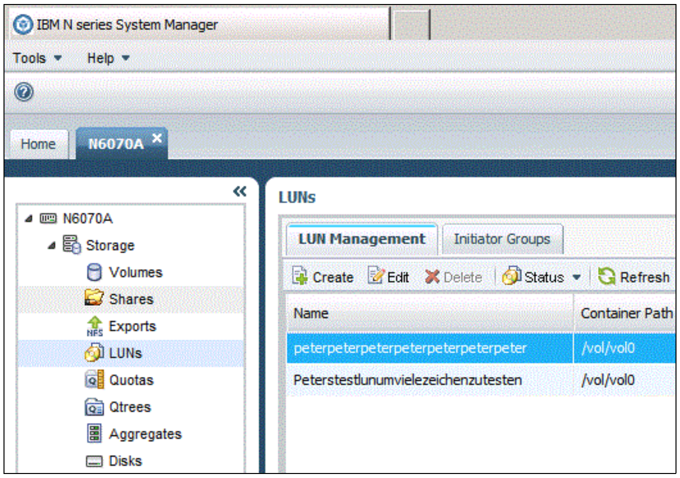
7.3.2 Creating a thin provisioned LUN on N series systems

To create a thin provisioned LUN, follow these steps:

1. Open IBM N series System Manager:

   `http://127.0.0.1:5718`

2. Open Storage, select **LUNs**, and then **Create** as shown in the **LUNs** pane (Figure 7-5).

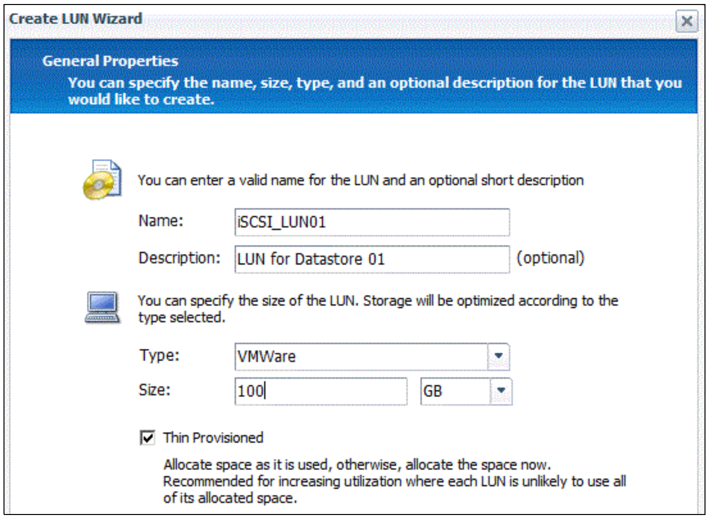


Name	Container Path
peterpeterpeterpeterpeterpeterpeter	/vol/vol0
Peterstestlunumvielezeichenzutesten	/vol/vol0

Figure 7-5 Creating a LUN

3. Add the following information, as shown in Figure 7-6, then click **Next**.

   a. **Name** to identify the LUN.
   b. **Description**.
   c. **Type** to define the LUN access method.
   d. **Size** of the LUN and its unit, as TB, GB, or MB.
   e. Thin Provisioned



General Properties

You can specify the name, size, type, and an optional description for the LUN that you would like to create.

You can enter a valid name for the LUN and an optional short description

Name: iSCSI_LUN01

Description: LUN for Datastore 01 (optional)

You can specify the size of the LUN. Storage will be optimized according to the type selected.

Type: VMWare

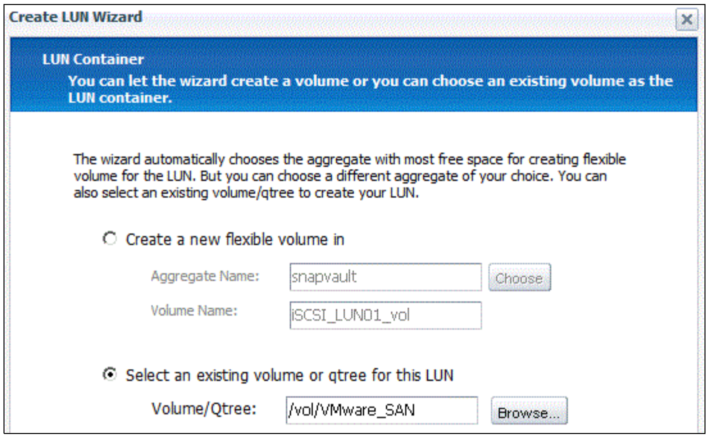
Size: 100 GB

☑ Thin Provisioned

Allocate space as it is used, otherwise, allocate the space now. Recommended for increasing utilization where each LUN is unlikely to use all of its allocated space.

Figure 7-6 Enter the requested information to create the LUN

4. In the next window, mark **Select an existing volume or qtree for this LUN**, and browse to select it, as shown in Figure 7-7.



LUN Container

You can let the wizard create a volume or you can choose an existing volume as the LUN container.

The wizard automatically chooses the aggregate with most free space for creating flexible volume for the LUN. But you can choose a different aggregate of your choice. You can also select an existing volume/qtree to create your LUN.

○ Create a new flexible volume in

Aggregate Name: snapvault

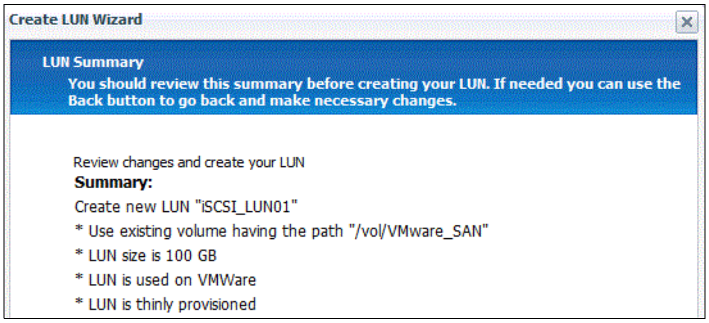
Volume Name: iSCSI_LUN01_vol

● Select an existing volume or qtree for this LUN

Volume/Qtree: /vol/VMware_SAN

Figure 7-7 Select the volume where the LUN will reside

5. In this example, we intend to map the LUN to an initiator later, so just click **Next** on the **Initiators Mapping** window.
6. On LUN Summary, review the information previously entered as shown in Figure 7-8 and click **Next**.



LUN Summary

You should review this summary before creating your LUN. If needed you can use the Back button to go back and make necessary changes.

Review changes and create your LUN

Summary:

Create new LUN "iSCSI_LUN01"

* Use existing volume having the path "/vol/VMware_SAN"

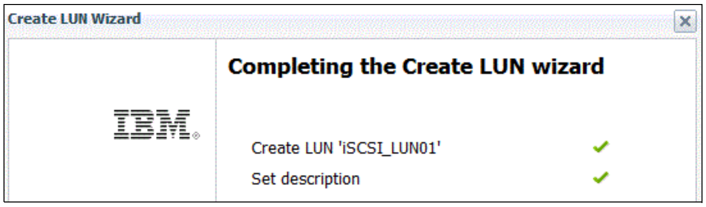
* LUN size is 100 GB

* LUN is used on VMWare

* LUN is thinly provisioned

Figure 7-8 LUN Summary review

7. If no error occur, a LUN will be created and the following information is displayed as shown in Figure 7-9. Click **Finish** to complete the process.



Completing the Create LUN wizard

Create LUN 'iSCSI_LUN01' ✓

Set description ✓

Figure 7-9 LUN creation success

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

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

Automatic grow this volume 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 it is nearly full. For VMware environments, set this value to On, which requires setting the maximum volume and increment size options.

Automatic delete older Snapshot copies 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 environments, set this value to delete Snapshot copies at 5% of available space. In addition, set the volume option to have the system attempting to grow the volume before deleting Snapshot copies.

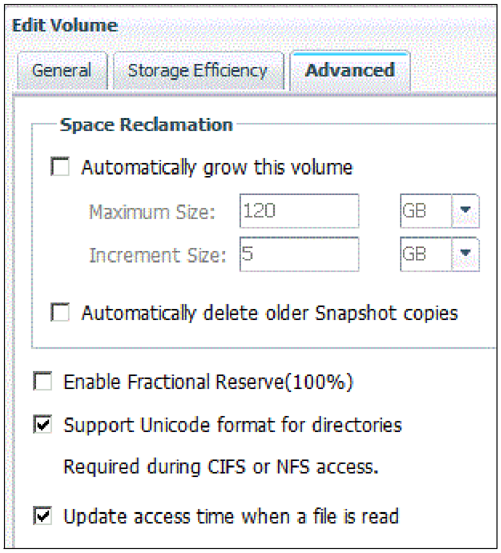
LUN Fractional Reserve is a required policy when using N series Snapshot copies on volumes that contain LUNs. This policy defines the amount of additional space reserved to guarantee LUN writes if a volume becomes 100% full. It works by avoiding a volume to take a Snapshot if the space available after that operation is not too low.

For VMware 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%.

Those settings can be set on the properties of the volume, on Advanced, as shown in Figure 7-10.



□ Automatically grow this volume

Maximum Size: 120 GB

Increment Size: 5 GB

□ Automatically delete older Snapshot copies

□ Enable Fractional Reserve(100%)

☑ Support Unicode format for directories

Required during CIFS or NFS access.

☑ Update access time when a file is read

Figure 7-10 Setting advanced volume options

7.3.3 Creating an initiator group on N series systems

To make a LUN visible to servers, create a initiator group as follows:

1. Navigate to **Storage** → **LUNs**, then select **Initiator Groups**, then select **Create**, as shown in Figure 7-11.

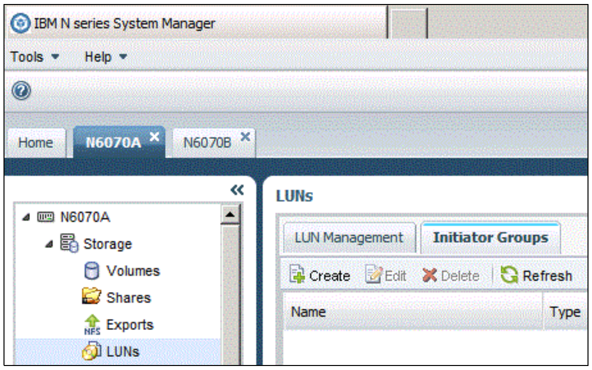
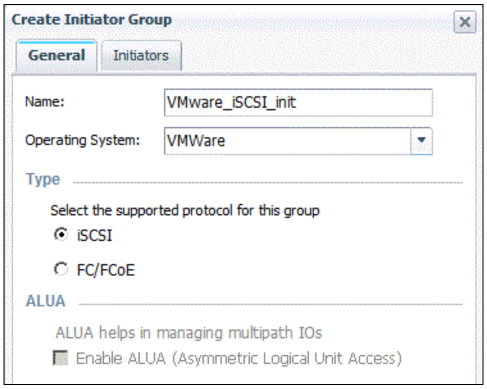


Figure 7-11 Creating an initiator group

2. On the General tab, type your information as shown in Figure 7-12.



Name: VMware_iSCSI_init

Operating System: VMWare

Type

Select the supported protocol for this group

● iSCSI

○ FC/FCoE

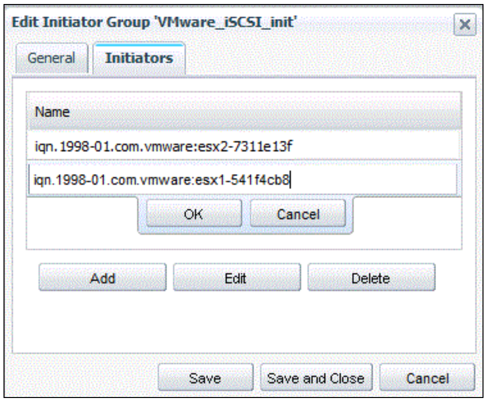
ALUA

ALUA helps in managing multipath IOs

□ Enable ALUA (Asymmetric Logical Unit Access)

Figure 7-12 Initiator Group creation

3. Click the **Initiators** tab and click **Add**, then type the IQN form each host. It should look like Figure 7-13. Click **Save and Close** and it will be ready.



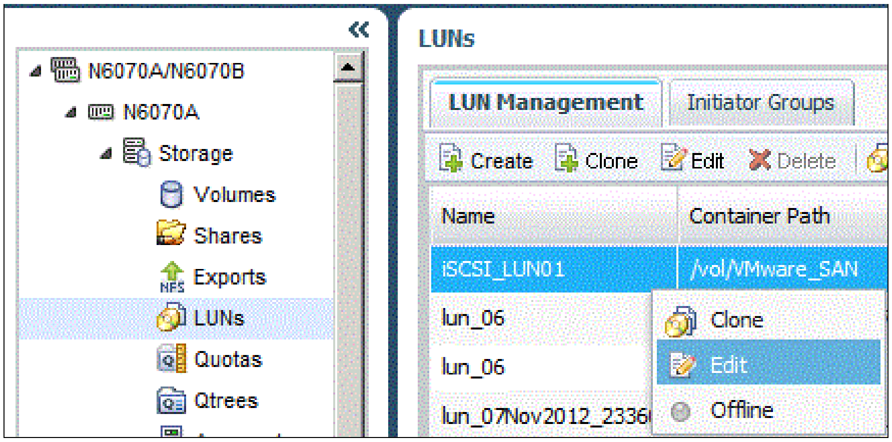
Name
iqn.1998-01.com.vmware:esx2-7311e13f
iqn.1998-01.com.vmware:esx1-541f4cb8

Figure 7-13 Adding IQNs from VMware host

7.3.4 Mapping a LUN to an initiator

Follow these steps:

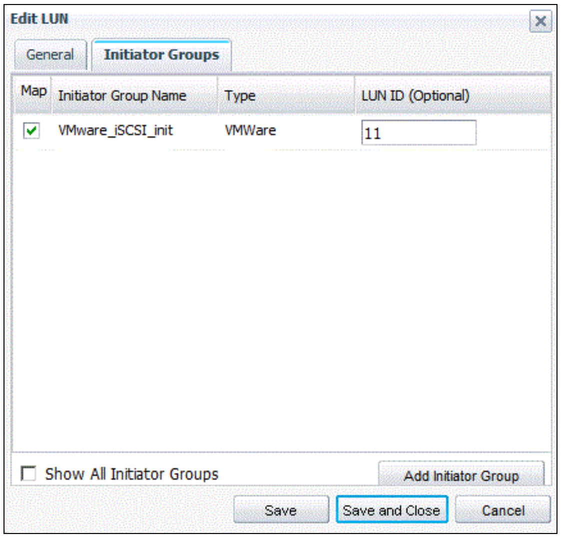
1. Click **LUNs**, right-click the LUN to be mapped, and click **Edit**, as shown in Figure 7-14.



Name	Container Path
iSCSI_LUN01	/vol/VMware_SAN
lun_06	
lun_06	
lun_07Nov2012_2336	

Figure 7-14 Editing the LUN to be mapped

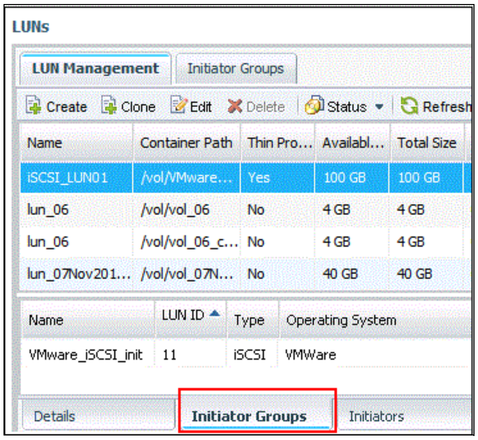
2. The **Edit LUN** window displays. Click **Initiator Groups**, mark the box referring to the Initiator to be used, Type, and LUN ID, as shown in Figure 7-15. Click **Save and Close**.



Map	Initiator Group Name	Type	LUN ID (Optional)
☑	VMware_iSCSI_init	VMWare	11

Figure 7-15 Select the box and enter a LUN ID on the Initiator Group entry

3. To check the existing mappings for a particular LUN, select it and click the **Initiators Groups** tab below the main panel, as shown in Figure 7-16.



Name	Container Path	Thin Pro...	Availabl...	Total Size
iSCSI_LUN01	/vol/VMware...	Yes	100 GB	100 GB
lun_06	/vol/vol_06	No	4 GB	4 GB
lun_06	/vol/vol_06_c...	No	4 GB	4 GB
lun_07Nov201...	/vol/vol_07N...	No	40 GB	40 GB

Name	LUN ID ▲	Type	Operating System
VMware_iSCSI_init	11	iSCSI	VMWare

Figure 7-16 Current mappings of a LUN

7.4 Presenting LUNs to an ESXi server over Fibre Channel

This section describes how to allocate a LUN to a host, so it can be used as a datastore and provide virtual disks for your virtual machines.

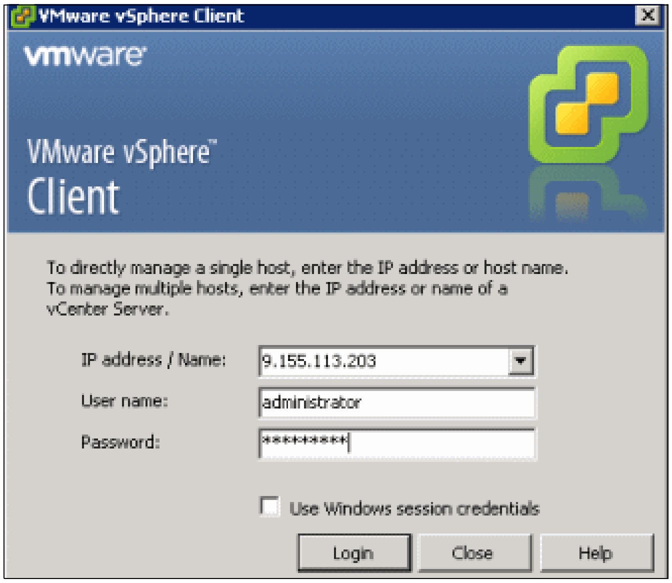
The storage limits were increased on VMware vSphere 5, making the storage and server administrators' environment easier to manage.

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

- LUN creation
- 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. Open the **Virtual Infrastructure Client** and point it to your vCenter IP, typing your user and password, as shown in Figure 7-17.



To directly manage a single host, enter the IP address or host name.
To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: 9.155.113.203

User name: administrator

Password: *********

□ Use Windows session credentials

Figure 7-17 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.

2. 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.

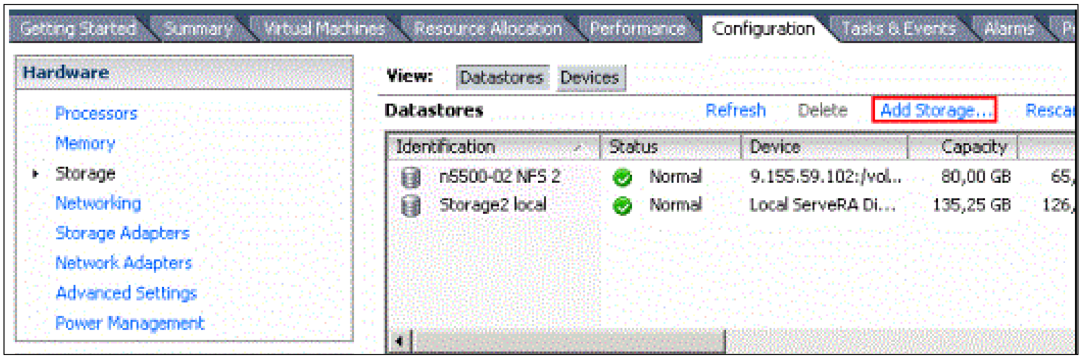
3. Repeat these steps for each host in the data center.

> **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:

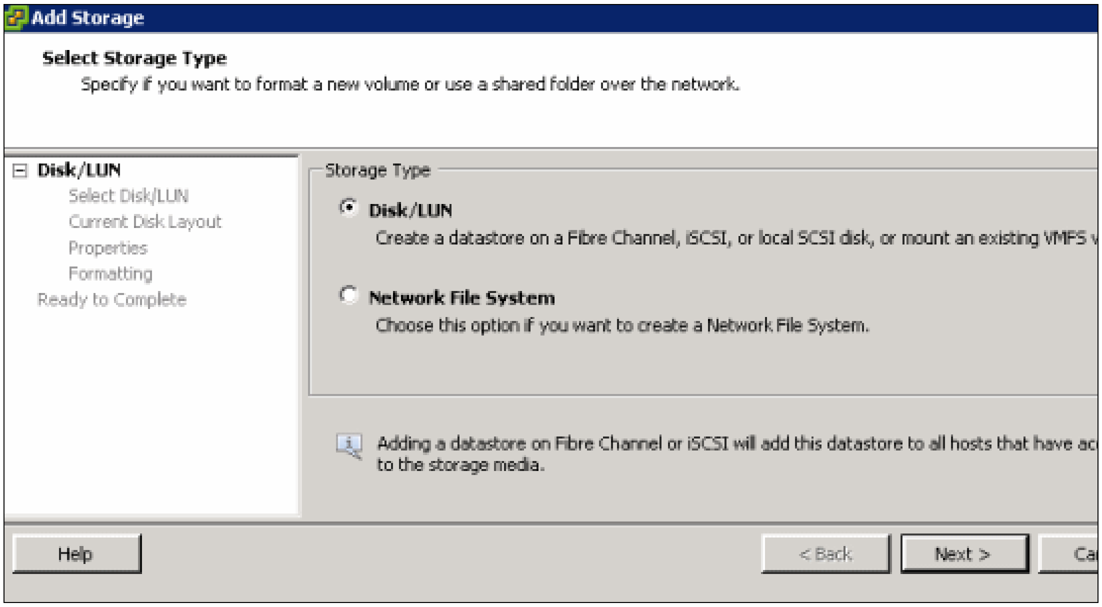
1. With vCenter opened, select a host.
2. In the right pane, select the **Configuration** tab.
3. In the Hardware box, select the **Storage** link and click **Add Storage**, as shown in Figure 7-18.



Identification	Status	Device	Capacity	
n5500-02 NFS 2	Normal	9.155.59.102:/vol...	80,00 GB	65,
Storage2 local	Normal	Local ServeRA Di...	135,25 GB	126,

Figure 7-18 Adding storage

4. In the Add Storage wizard (Figure 7-19), select the **Disk/LUN** radio button and click **Next**.



Add Storage

Select Storage Type

Specify if you want to format a new volume or use a shared folder over the network.

- Disk/LUN
  - Select Disk/LUN
  - Current Disk Layout
  - Properties
  - Formatting
- Ready to Complete

Storage Type

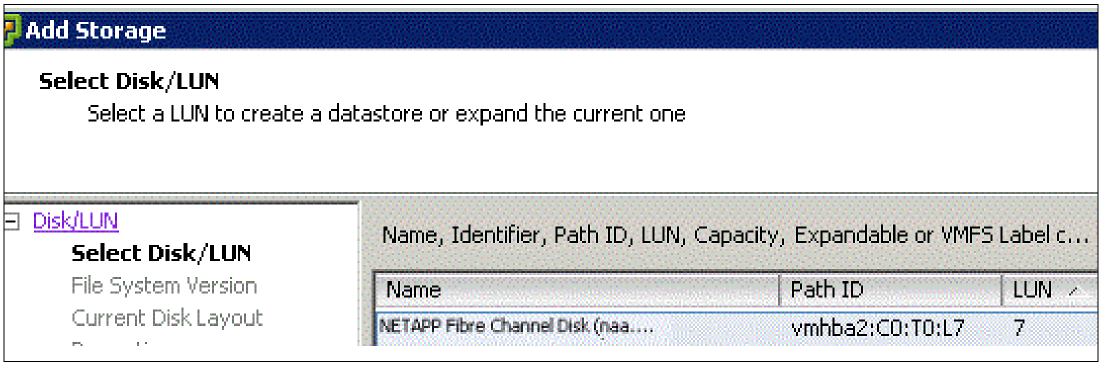
● **Disk/LUN**
Create a datastore on a Fibre Channel, iSCSI, or local SCSI disk, or mount an existing VMFS v

○ **Network File System**
Choose this option if you want to create a Network File System.

Adding a datastore on Fibre Channel or iSCSI will add this datastore to all hosts that have ac to the storage media.

Figure 7-19 Add Storage wizard

5. Select the LUN that you want to use and click **Next** (Figure 7-20).



Add Storage

Select Disk/LUN

Select a LUN to create a datastore or expand the current one

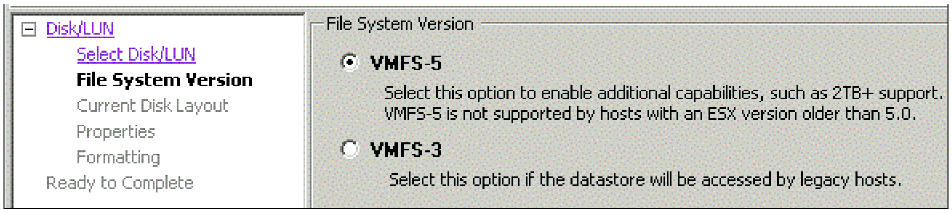
- Disk/LUN
  - **Select Disk/LUN**
  - File System Version
  - Current Disk Layout

Name, Identifier, Path ID, LUN, Capacity, Expandable or VMFS Label c...

Name	Path ID	LUN
NETAPP Fibre Channel Disk (naa....	vmhba2:C0:T0:L7	7

Figure 7-20 Selecting a LUN

6. Since VMware ESXi 5, the block size of a new created datastore has been changed to 1 MB, while maintaining the limit of 2 TB as the maximum file size, which means that the VM's disks are still limited to that size. If your infrastructure runs a mix of ESXi 5 and previous versions, it is desirable to create the datastores with VMFS-3, and VMFS-5 does not have backward compatibility. Figure 7-21 shows that selection window. Then click **Next**.



- Disk/LUN
  - Select Disk/LUN
  - **File System Version**
  - Current Disk Layout
  - Properties
  - Formatting
- Ready to Complete

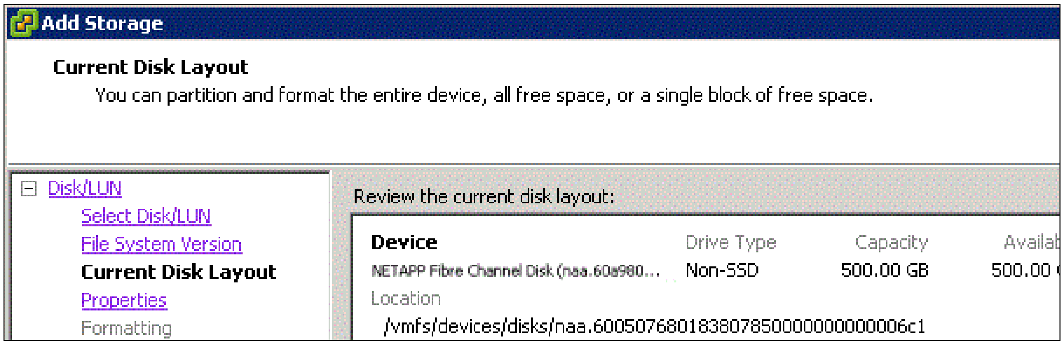
File System Version

● **VMFS-5**
Select this option to enable additional capabilities, such as 2TB+ support.
VMFS-5 is not supported by hosts with an ESX version older than 5.0.

○ **VMFS-3**
Select this option if the datastore will be accessed by legacy hosts.

Figure 7-21 Datastore compatibility selection

7. View the selected LUN information as shown in Figure 7-22 and click **Next**.


Add Storage

Current Disk Layout

You can partition and format the entire device, all free space, or a single block of free space.

Review the current disk layout:

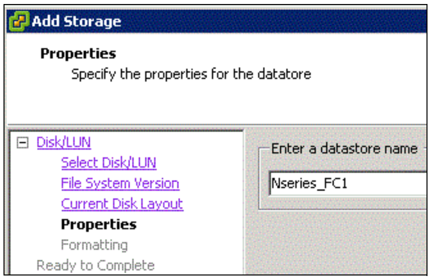
Device	Drive Type	Capacity	Availab
NETAPP Fibre Channel Disk (naa.60a980...	Non-SSD	500.00 GB	500.00

Location

/vmfs/devices/disks/naa.600507680183807850000000000006c1

Figure 7-22 LUN information

8. Type a name for the datastore as shown in Figure 7-23 and click **Next**.


Add Storage

Properties

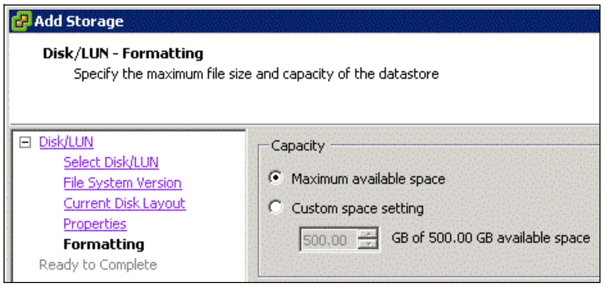
Specify the properties for the datatore

Enter a datastore name

Nseries_FC1

Figure 7-23 Define datastore name

9. Select if you want use all the LUN space by selecting **Maximum available space**, or select a different value on the **Custom space setting** as shown in Figure 7-24, then click **Next**.Unless you have a technical reason not to, select **Maximum available space**.


Add Storage

Disk/LUN - Formatting

Specify the maximum file size and capacity of the datastore

Capacity

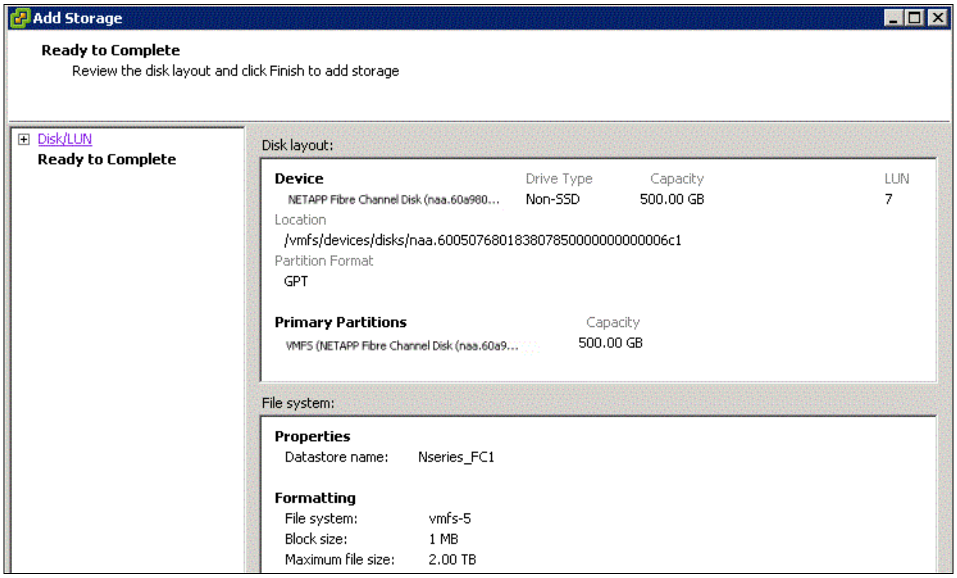
● Maximum available space

○ Custom space setting

500.00 GB of 500.00 GB available space

Figure 7-24 Selecting how much space of a LUN the datastore will take

10. Review the information entered and click as shown in Figure 7-25, and then click **Finish**.



Add Storage

Ready to Complete
Review the disk layout and click Finish to add storage

Disk/LUN
Ready to Complete

Disk layout:

Device	Drive Type	Capacity	LUN
NETAPP Fibre Channel Disk (naa.60a980...	Non-SSD	500.00 GB	7

Location
/vmfs/devices/disks/naa.600507680183807850000000000006c1

Partition Format
GPT

Primary Partitions	Capacity
VMFS (NETAPP Fibre Channel Disk (naa.60a9...	500.00 GB

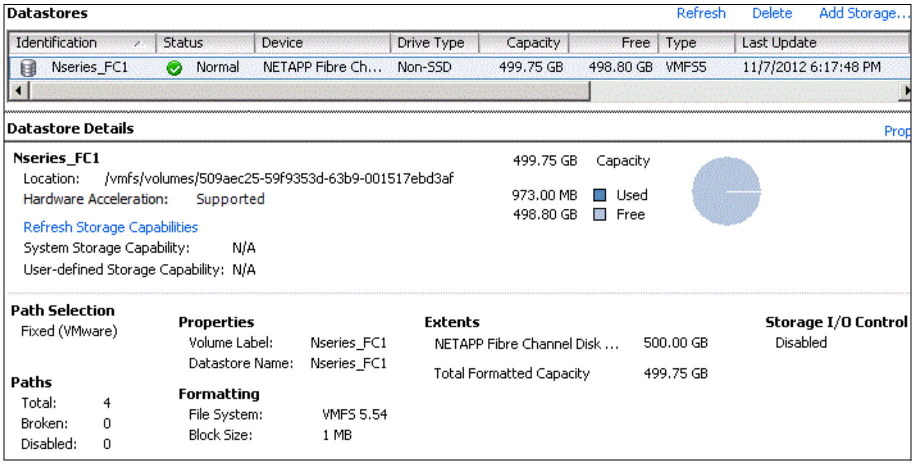
File system:

Properties
Datastore name: Nseries_FC1

Formatting
File system: vmfs-5
Block size: 1 MB
Maximum file size: 2.00 TB

Figure 7-25 Reviewing datastore creation information.

11. After its creation, clicking the datastore will show details (see Figure 7-26).



Datastores

Identification	Status	Device	Drive Type	Capacity	Free	Type	Last Update
Nseries_FC1	✓ Normal	NETAPP Fibre Ch...	Non-SSD	499.75 GB	498.80 GB	VMFS5	11/7/2012 6:17:48 PM

Datastore Details

Nseries_FC1
Location: /vmfs/volumes/509aec25-59f9353d-63b9-001517ebd3af
Hardware Acceleration: Supported

Refresh Storage Capabilities
System Storage Capability: N/A
User-defined Storage Capability: N/A

499.75 GB Capacity
973.00 MB ■ Used
498.80 GB □ Free

Path Selection
Fixed (VMware)

Paths
Total: 4
Broken: 0
Disabled: 0

Properties
Volume Label: Nseries_FC1
Datastore Name: Nseries_FC1

Formatting
File System: VMFS 5.54
Block Size: 1 MB

Extents
NETAPP Fibre Channel Disk ... 500.00 GB
Total Formatted Capacity 499.75 GB

Storage I/O Control
Disabled

Figure 7-26 Datastore information

7.5 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* to access to the external storage system. With dynamic name resolution, it can use 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 on 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 cluster where the VM‘s data resides on external storage device. You can only use RDM over the Fibre Channel.

7.5.1 RDM compatibility mode

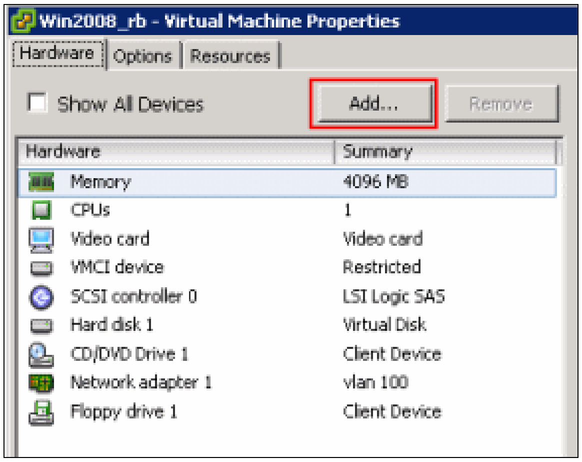
RDM devices can be used in virtual or physical mode:

- With virtual mode, you can use raw disks to get 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. This mode is required when using for a Microsoft cluster solution where the VMs could run on any ESXi host. However, when using physical mode, you lose the ability to use Snapshot or vMotion that VM while it is powered on to another physical host.

7.5.2 Attaching an RDM disk device to a virtual machine

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

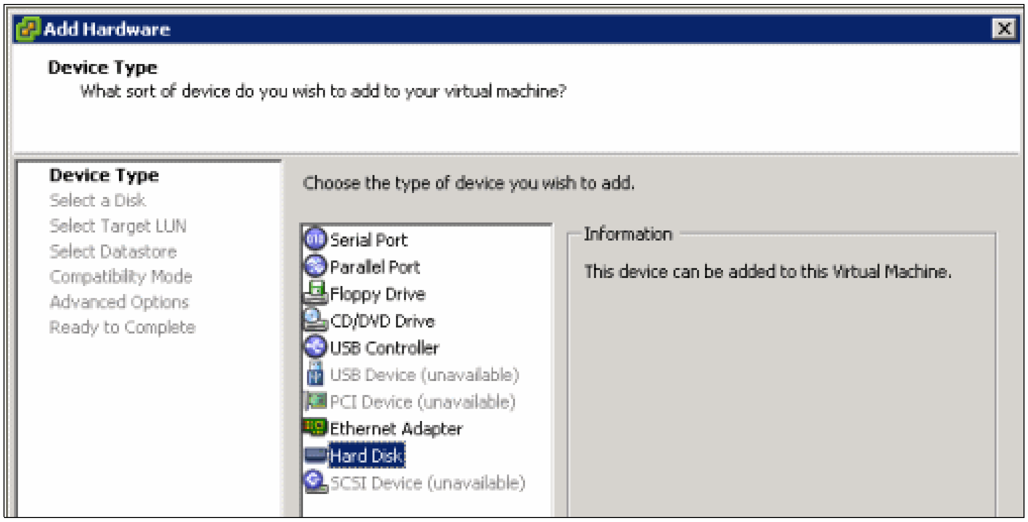
1. Have a LUN available and mapped to be used into a virtual machine.
2. Go to the Virtual Infrastructure Client and rescan the host where that VM resides so it can see that available LUN. On the **Configuration** tab, select the **Storage adapters**, and then click **Rescan**.
3. Right-click the VM to which you want to add the RDM device, and click **Edit Settings**.
4. Click **Add** as shown in Figure 7-27.



Hardware	Summary
Memory	4096 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
CD/DVD Drive 1	Client Device
Network adapter 1	vlan 100
Floppy drive 1	Client Device

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**.


Add Hardware

Device Type

What sort of device do you wish to add to your virtual machine?

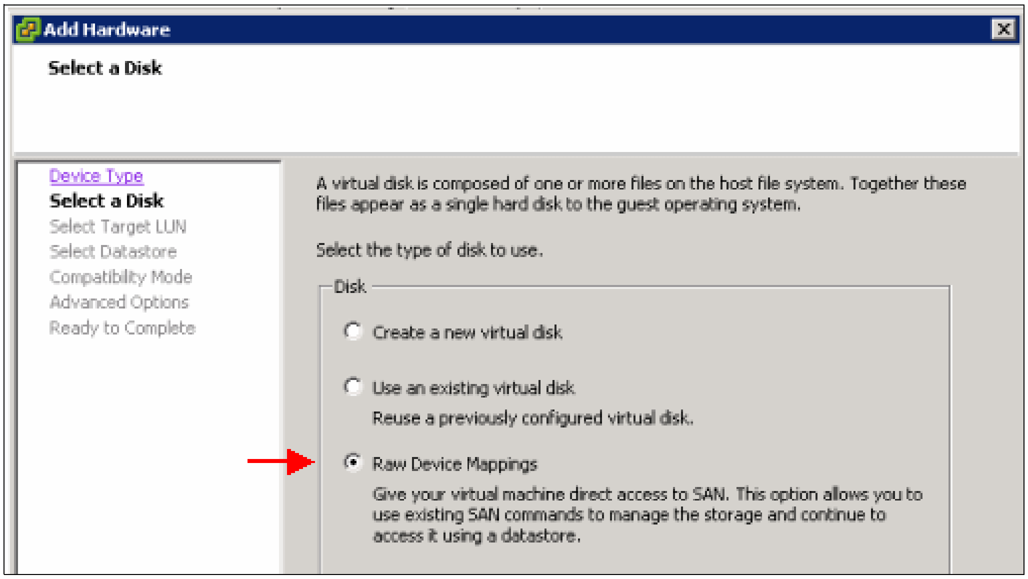
Choose the type of device you wish to add.

Information

This device can be added to this Virtual Machine.

Figure 7-28 Adding a new hard disk

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


Add Hardware

Select a Disk

A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system.

Select the type of disk to use.

Disk

○ Create a new virtual disk

○ Use an existing virtual disk

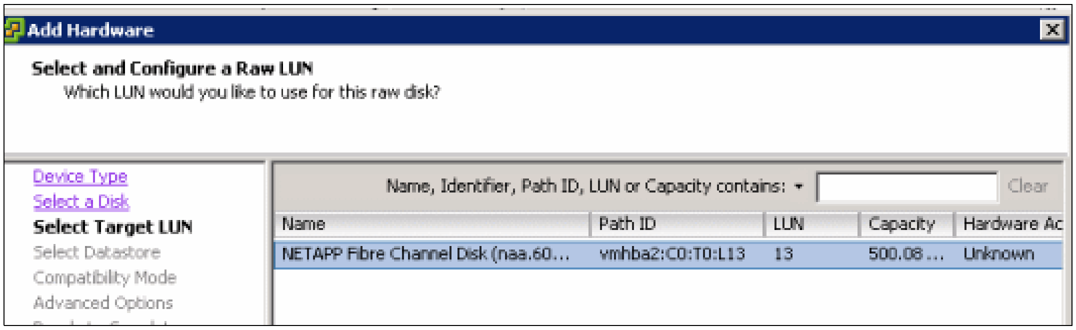
Reuse a previously configured virtual disk.

● Raw Device Mappings

Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.

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**.


Add Hardware

Select and Configure a Raw LUN

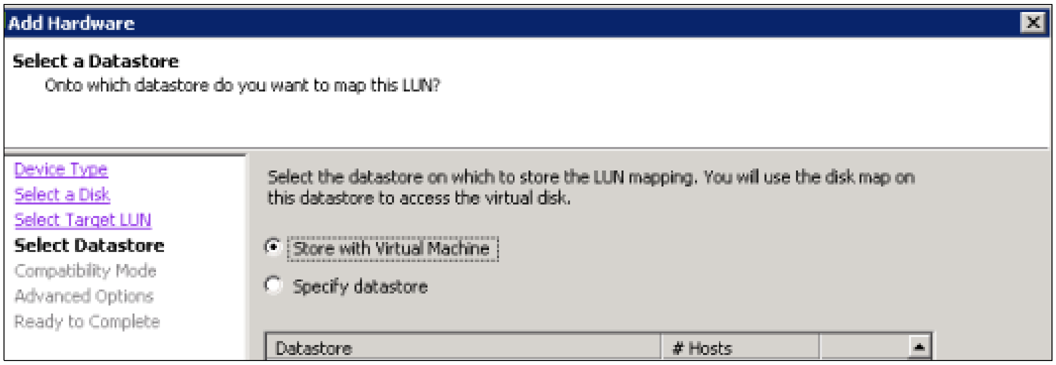
Which LUN would you like to use for this raw disk?

Name, Identifier, Path ID, LUN or Capacity contains:

Name	Path ID	LUN	Capacity	Hardware Ac
NETAPP Fibre Channel Disk (naa.60...	vmhba2:C0:T0:L13	13	500.08 ...	Unknown

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 on another VMFS datastore, then click **Next**.



Add Hardware

Select a Datastore
Onto which datastore do you want to map this LUN?

Select the datastore on which to store the LUN mapping. You will use the disk map on this datastore to access the virtual disk.

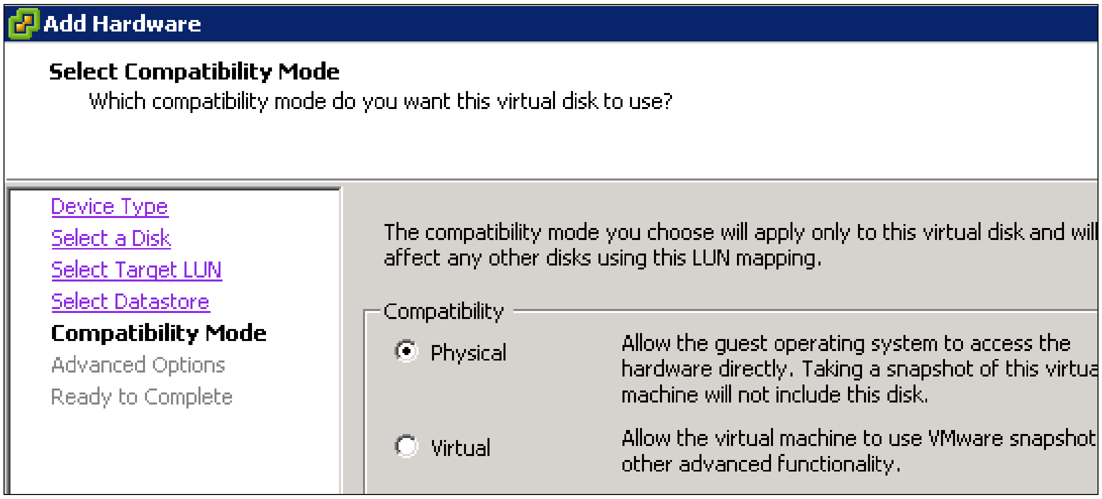
● Store with Virtual Machine

○ Specify datastore

Datastore	# Hosts

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 7.5.1, “RDM compatibility mode” on page 113. Click **Next**.



Add Hardware

Select Compatibility Mode
Which compatibility mode do you want this virtual disk to use?

The compatibility mode you choose will apply only to this virtual disk and will affect any other disks using this LUN mapping.

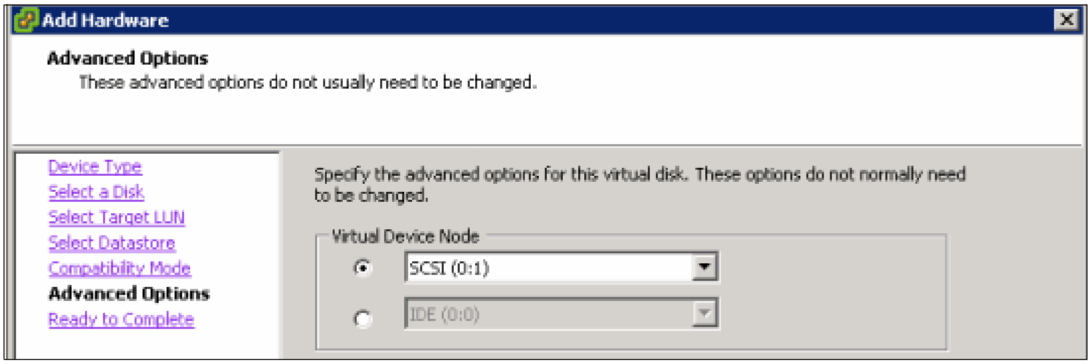
Compatibility

● Physical — Allow the guest operating system to access the hardware directly. Taking a snapshot of this virtua machine will not include this disk.

○ Virtual — Allow the virtual machine to use VMware snapshot other advanced functionality.

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. If none change is needed, accept the default options and click **Next**.



Add Hardware

Advanced Options
These advanced options do not usually need to be changed.

Specify the advanced options for this virtual disk. These options do not normally need to be changed.

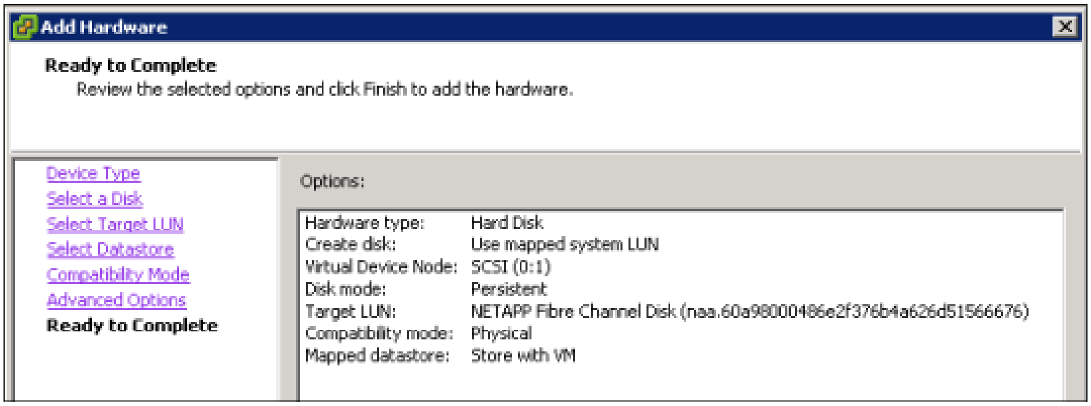
Virtual Device Node

● SCSI (0:1)

○ IDE (0:0)

Figure 7-33 Specifying the advanced options

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



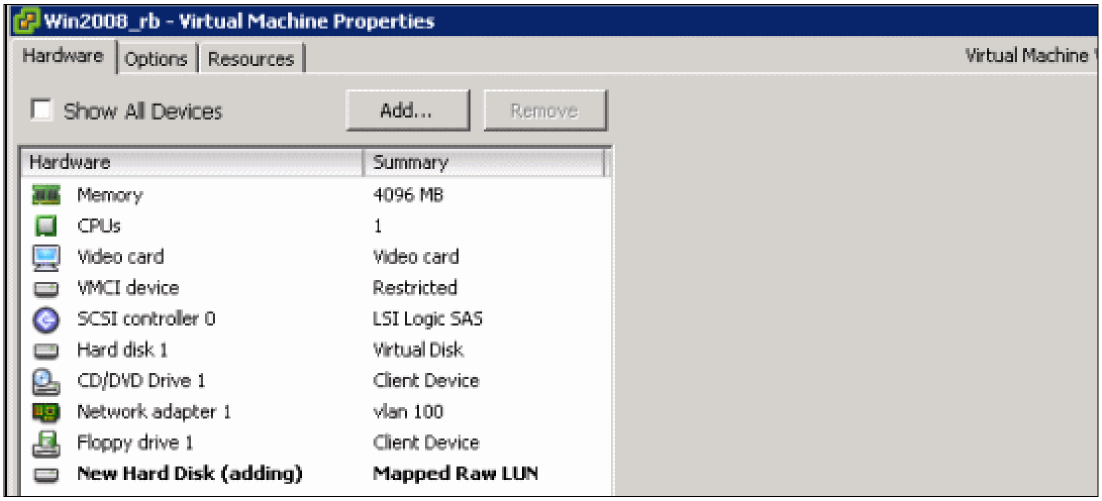
Ready to Complete
Review the selected options and click Finish to add the hardware.

Options:

Hardware type:	Hard Disk
Create disk:	Use mapped system LUN
Virtual Device Node:	SCSI (0:1)
Disk mode:	Persistent
Target LUN:	NETAPP Fibre Channel Disk (naa.60a98000486e2f376b4a626d51566676)
Compatibility mode:	Physical
Mapped datastore:	Store with VM

Figure 7-34 Summary of settings

12. After the wizard finishes, the RDM can be seen on the VM's properties (Figure 7-35). Click **OK** to finish the process. The virtual machine is ready to use the RDM device.



Hardware	Summary
Memory	4096 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
CD/DVD Drive 1	Client Device
Network adapter 1	vlan 100
Floppy drive 1	Client Device
New Hard Disk (adding)	**Mapped Raw LUN**

Figure 7-35 RDM hard disk attached

7.6 Creating a VMKernel portgroup on VMware vSphere 5.1

In order to communicate to a storage using the network (iSCSI and NFS, 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 to avoid bottlenecks from one to interfere on another.

To configure the storage network connectivity, complete the following 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 shown in Figure 7-36.

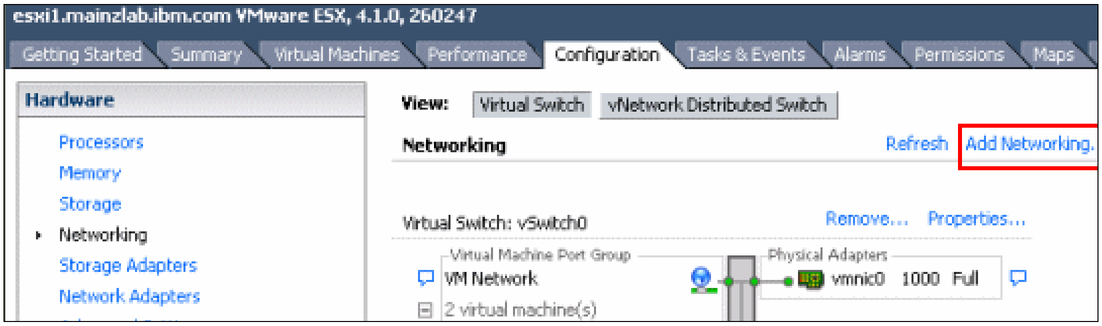
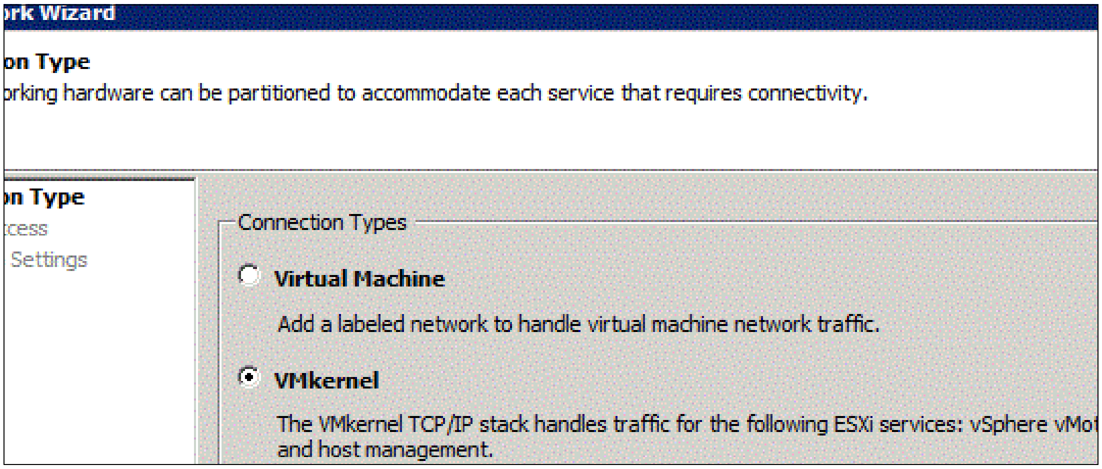


Figure 7-36 Adding network

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



rk Wizard

on Type

rking hardware can be partitioned to accommodate each service that requires connectivity.

n Type
cess
Settings

Connection Types

○ **Virtual Machine**

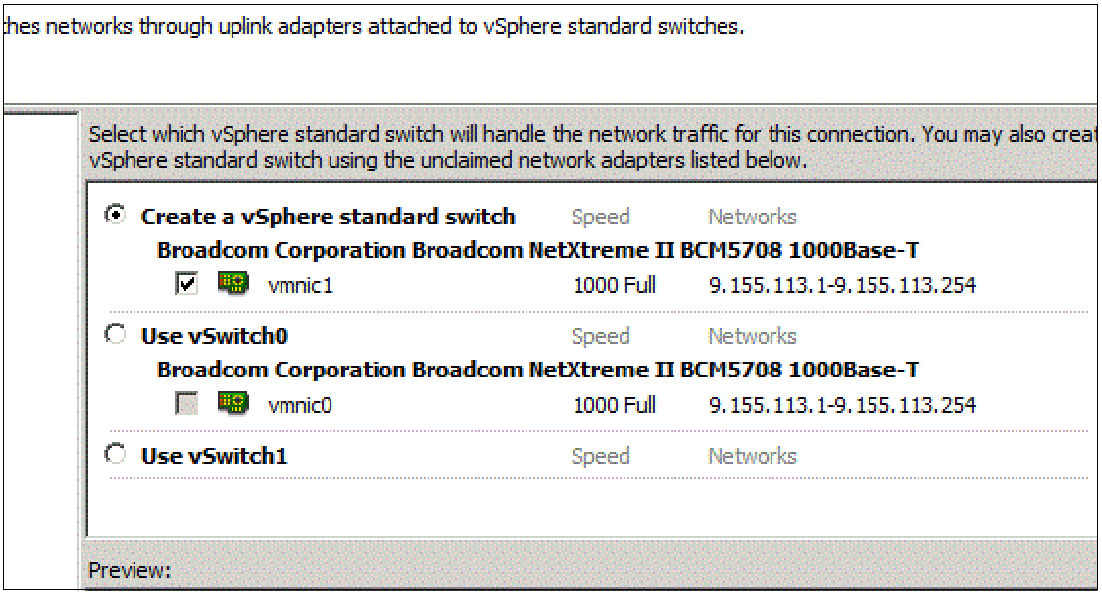
Add a labeled network to handle virtual machine network traffic.

● **VMkernel**

The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMo
and host management.

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.



hes networks through uplink adapters attached to vSphere standard switches.

Select which vSphere standard switch will handle the network traffic for this connection. You may also creat
vSphere standard switch using the unclaimed network adapters listed below.

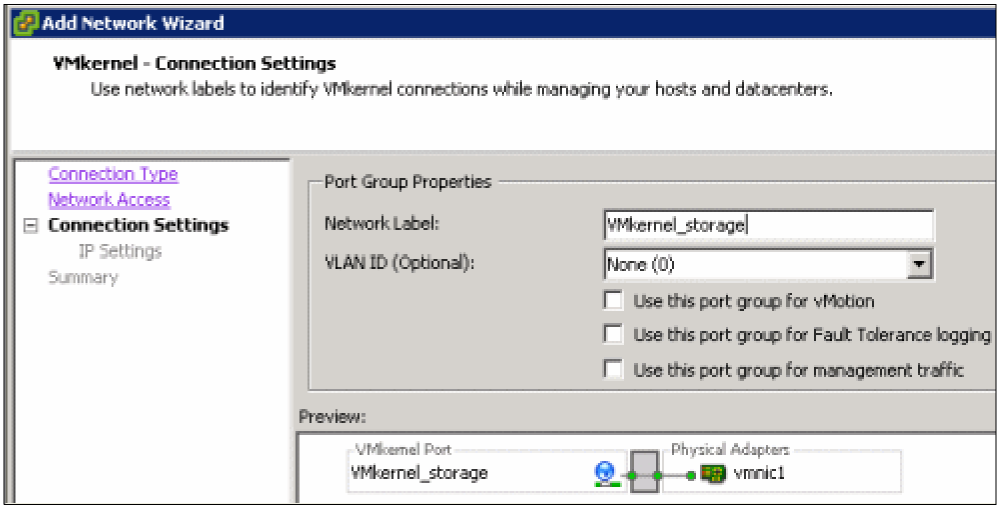
	Speed	Networks
● **Create a vSphere standard switch**	Speed	Networks
Broadcom Corporation Broadcom NetXtreme II BCM5708 1000Base-T		
☑ vmnic1	1000 Full	9.155.113.1-9.155.113.254
○ **Use vSwitch0**	Speed	Networks
Broadcom Corporation Broadcom NetXtreme II BCM5708 1000Base-T		
□ vmnic0	1000 Full	9.155.113.1-9.155.113.254
○ **Use vSwitch1**	Speed	Networks

Preview:

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 shown in Figure 7-39.



VMkernel - Connection Settings

Use network labels to identify VMkernel connections while managing your hosts and datacenters.

Port Group Properties

Network Label: VMkernel_storage

VLAN ID (Optional): None (0)

□ Use this port group for vMotion

□ Use this port group for Fault Tolerance logging

□ Use this port group for management traffic

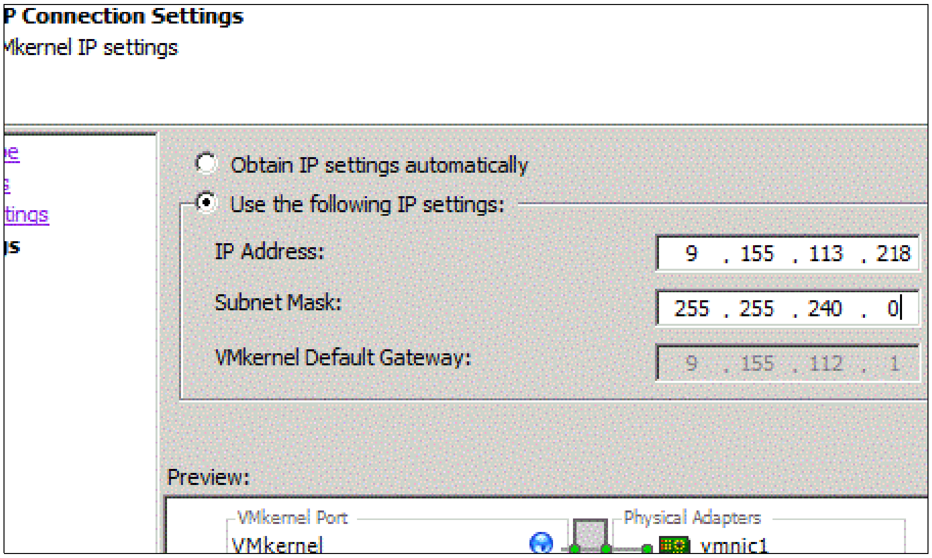
Preview:

VMkernel Port: VMkernel_storage

Physical Adapters: vmnic1

Figure 7-39 Naming the portgroup

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



P Connection Settings

Mkernel IP settings

○ Obtain IP settings automatically

● Use the following IP settings:

IP Address: 9 . 155 . 113 . 218

Subnet Mask: 255 . 255 . 240 . 0

VMkernel Default Gateway: 9 . 155 . 112 . 1

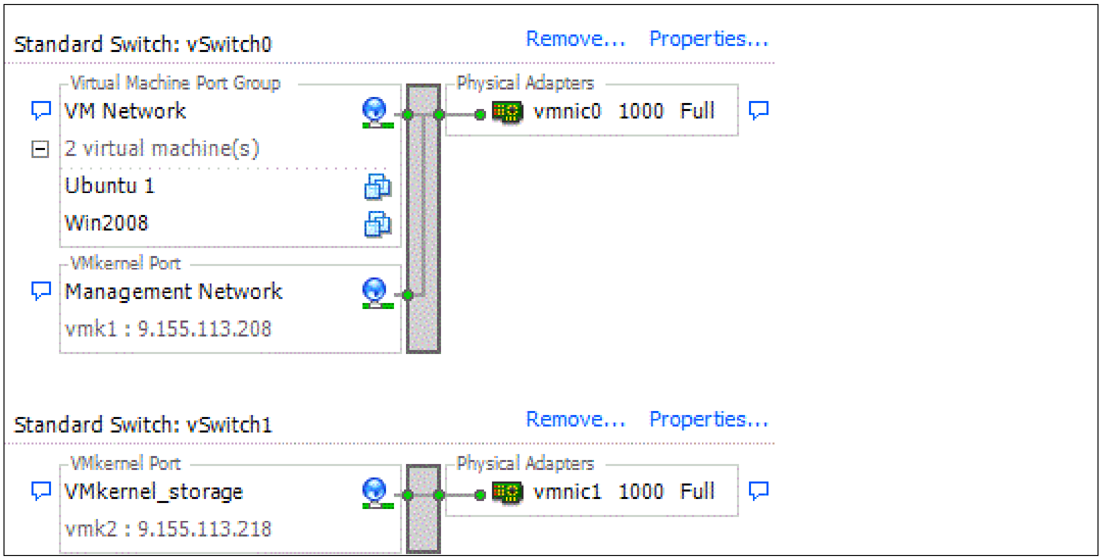
Preview:

VMkernel Port: VMkernel

Physical Adapters: vmnic1

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.



Standard Switch: vSwitch0

VM Network
2 virtual machine(s)
Ubuntu 1
Win2008

Management Network
vmk1 : 9.155.113.208

vmnic0 1000 Full

Standard Switch: vSwitch1

VMkernel_storage
vmk2 : 9.155.113.218

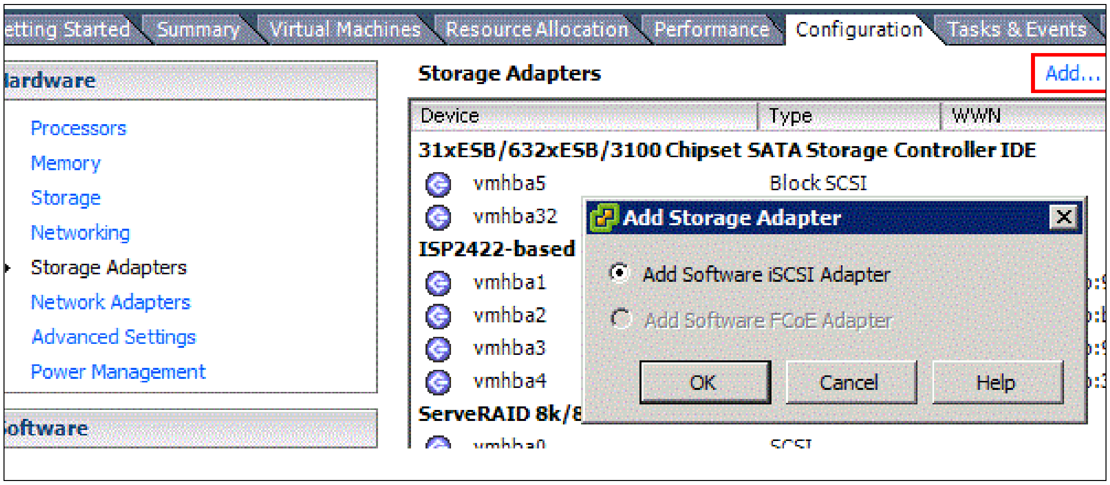
vmnic1 1000 Full

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

7.7 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. On ESXi, click the host to have the iSCSI configured, then go to the **Configuration** tab. Select **Storage Adapters in the** left panel, then click **Add**, as shown in Figure 7-42.



Storage Adapters

Device	Type	WWN
31xESB/632xESB/3100 Chipset SATA Storage Controller IDE		
vmhba5	Block SCSI	
vmhba32		
ISP2422-based		
vmhba1		
vmhba2		
vmhba3		
vmhba4		
ServeRAID 8k/8		
vmhba0	SCSI	

Add Storage Adapter

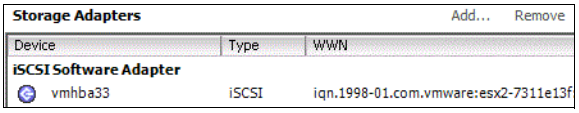
● Add Software iSCSI Adapter

○ Add Software FCoE Adapter

Figure 7-42 Selecting an iSCSI initiator

2. A warning will display stating that a software iSCSI adapter is about to be added. Click **OK** to proceed.

3. After completion, a iSCSI adapter will be available to be configured, as shown in Figure 7-43. Select it and then click **Properties...**

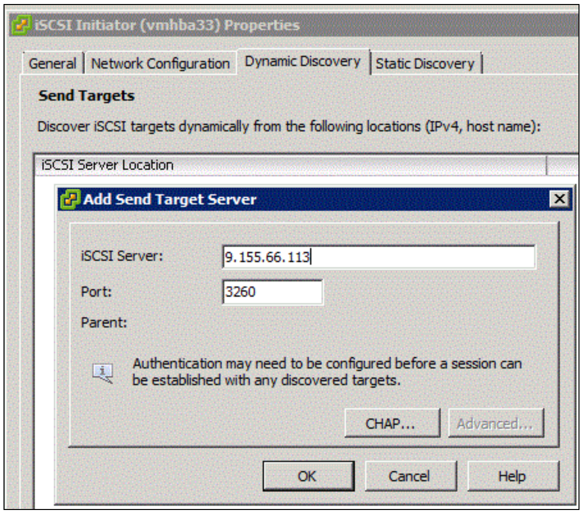


Storage Adapters Add... Remove

Device	Type	WWN
iSCSI Software Adapter		
vmhba33	iSCSI	iqn.1998-01.com.vmware:esx2-7311e13f

Figure 7-43 iSCSI software adapter

4. On the iSCSI initiator properties, click the **Dynamic Discovery** tab, then click **Add** and enter the storage port IP, as shown in Figure 7-44. Configure the CHAP authentication if suits to your environment, but be aware that it will add a layer of processing on the storage communication. It is a best practice as well as a better performing solution to keep the communication between hosts and storage on an isolated network.



iSCSI Initiator (vmhba33) Properties

General | Network Configuration | Dynamic Discovery | Static Discovery

Send Targets

Discover iSCSI targets dynamically from the following locations (IPv4, host name):

iSCSI Server Location

Add Send Target Server

iSCSI Server: 9.155.66.113

Port: 3260

Parent:

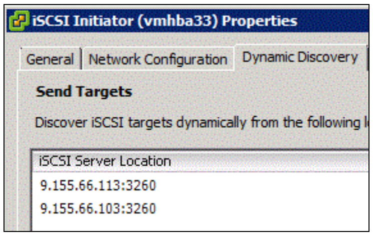
Authentication may need to be configured before a session can be established with any discovered targets.

CHAP... Advanced...

OK Cancel Help

Figure 7-44 Adding iSCSI target to the interface

5. After repeating the previous step for all the storage targets, the iSCSI Dynamic Discovery might look as shown in Figure 7-45. Click **Close** and then click **OK** when asked to rescan the adapters.



iSCSI Initiator (vmhba33) Properties

General | Network Configuration | Dynamic Discovery

Send Targets

Discover iSCSI targets dynamically from the following l

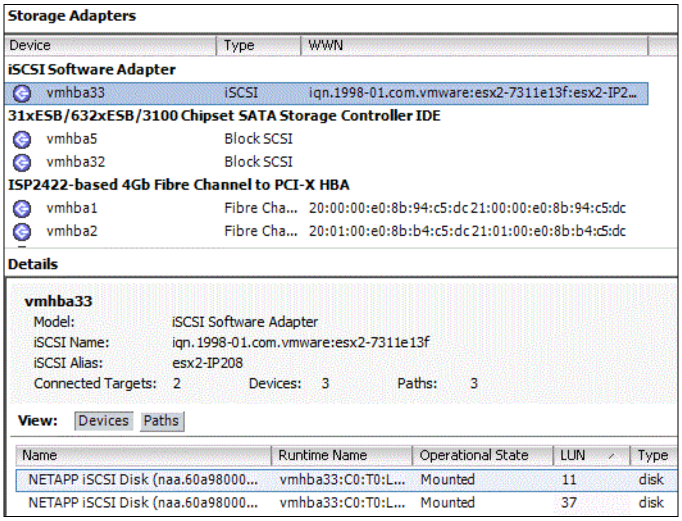
iSCSI Server Location

9.155.66.113:3260

9.155.66.103:3260

Figure 7-45 iSCSI targets on software iSCSI adapter

6. After the scan completes, all the LUNs assigned to that iSCSI adapter will be visible, as shown in Figure 7-46.



Storage Adapters

Device	Type	WWN
iSCSI Software Adapter		
vmhba33	iSCSI	iqn.1998-01.com.vmware:esx2-7311e13f:esx2-IP2...
31xESB/632xESB/3100 Chipset SATA Storage Controller IDE		
vmhba5	Block SCSI	
vmhba32	Block SCSI	
ISP2422-based 4Gb Fibre Channel to PCI-X HBA		
vmhba1	Fibre Cha...	20:00:00:e0:8b:94:c5:dc 21:00:00:e0:8b:94:c5:dc
vmhba2	Fibre Cha...	20:01:00:e0:8b:b4:c5:dc 21:01:00:e0:8b:b4:c5:dc

Details

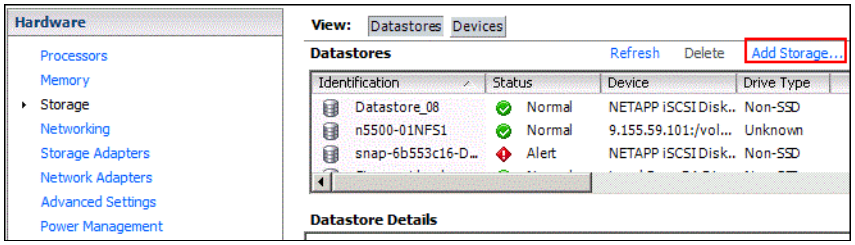
vmhba33
Model: iSCSI Software Adapter
iSCSI Name: iqn.1998-01.com.vmware:esx2-7311e13f
iSCSI Alias: esx2-IP208
Connected Targets: 2 Devices: 3 Paths: 3

View: Devices Paths

Name	Runtime Name	Operational State	LUN	Type
NETAPP iSCSI Disk (naa.60a98000...	vmhba33:C0:T0:L...	Mounted	11	disk
NETAPP iSCSI Disk (naa.60a98000...	vmhba33:C0:T0:L...	Mounted	37	disk

Figure 7-46 LUNs displaying after rescan

7. Go to Storage link and select **Add storage**, as shown in Figure 7-47.

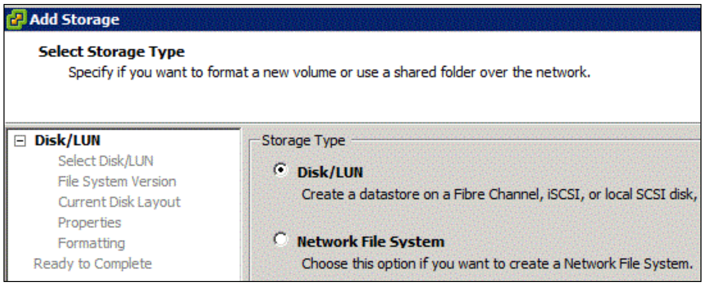


Datastores

Identification	Status	Device	Drive Type
Datastore_08	Normal	NETAPP iSCSI Disk..	Non-SSD
n5500-01NFS1	Normal	9.155.59.101:/vol...	Unknown
snap-6b553c16-D...	Alert	NETAPP iSCSI Disk..	Non-SSD

Figure 7-47 Adding Storage

8. Select **Disk/LUN** as shown in Figure 7-48 and click **Next**.



Select Storage Type
Specify if you want to format a new volume or use a shared folder over the network.

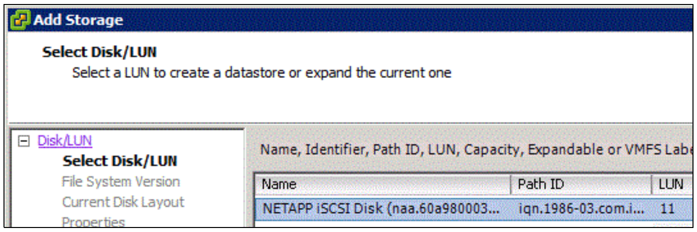
Storage Type

● **Disk/LUN**
Create a datastore on a Fibre Channel, iSCSI, or local SCSI disk,

○ **Network File System**
Choose this option if you want to create a Network File System.

Figure 7-48 Selecting access method

9. Select the LUN used as shown in Figure 7-49 and click **Next**.



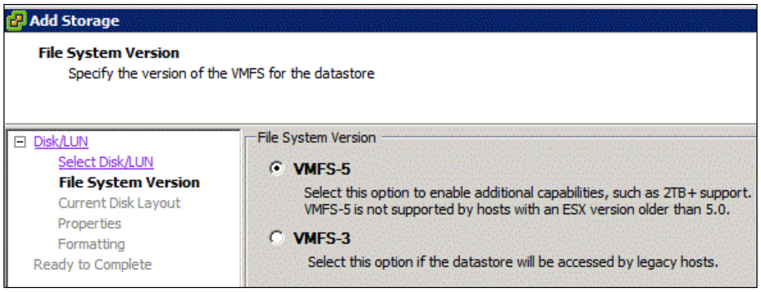
Select Disk/LUN
Select a LUN to create a datastore or expand the current one

Name, Identifier, Path ID, LUN, Capacity, Expandable or VMFS Labe

Name	Path ID	LUN
NETAPP iSCSI Disk (naa.60a980003...	iqn.1986-03.com.i...	11

Figure 7-49 Selecting LUN

10. Select the File System version as shown in Figure 7-50 and click **Next**.



File System Version

Specify the version of the VMFS for the datastore

File System Version

● VMFS-5

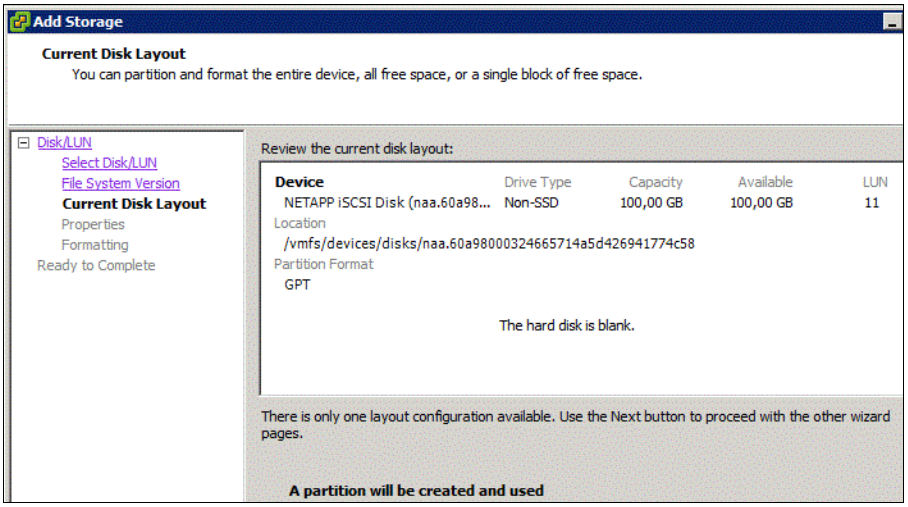
Select this option to enable additional capabilities, such as 2TB+ support. VMFS-5 is not supported by hosts with an ESX version older than 5.0.

○ VMFS-3

Select this option if the datastore will be accessed by legacy hosts.

Figure 7-50 Selecting file system

11. Review the LUN information as shown in Figure 7-51 and click **Next**.



Current Disk Layout

You can partition and format the entire device, all free space, or a single block of free space.

Review the current disk layout:

Device	Drive Type	Capacity	Available	LUN
NETAPP iSCSI Disk (naa.60a98...	Non-SSD	100,00 GB	100,00 GB	11

Location

/vmfs/devices/disks/naa.60a98000324665714a5d426941774c58

Partition Format

GPT

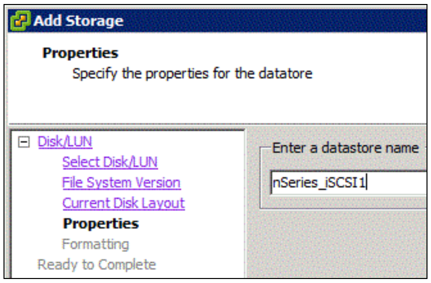
The hard disk is blank.

There is only one layout configuration available. Use the Next button to proceed with the other wizard pages.

A partition will be created and used

Figure 7-51 LUN information

12. Enter a name for the datastore as shown in Figure 7-52.



Properties

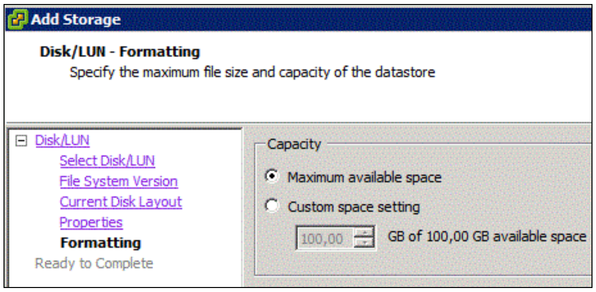
Specify the properties for the datatore

Enter a datastore name

nSeries_iSCSI1

Figure 7-52 Naming the datastore

13. Select if the datastore will take the entire LUN space selecting **Maximum available space** or enter the desired value as shown in Figure 7-53.



Add Storage

Disk/LUN - Formatting
Specify the maximum file size and capacity of the datastore

- Disk/LUN
  - Select Disk/LUN
  - File System Version
  - Current Disk Layout
  - Properties
  - **Formatting**
- Ready to Complete

Capacity

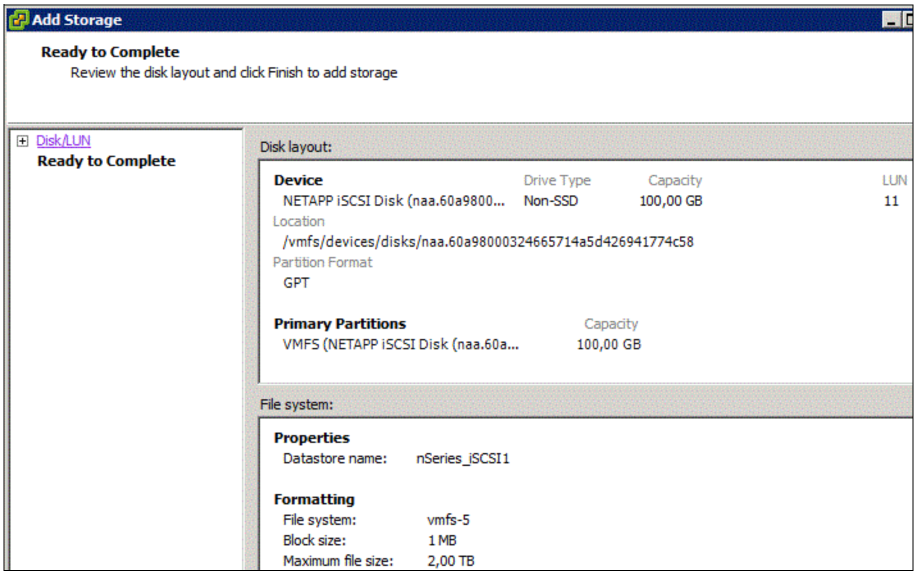
● Maximum available space

○ Custom space setting

100,00 GB of 100,00 GB available space

Figure 7-53 Selecting datastore size

14. Review the information and click **Finish** as shown in Figure 7-54.



Add Storage

Ready to Complete
Review the disk layout and click Finish to add storage

- Disk/LUN
- **Ready to Complete**

Disk layout:

Device	Drive Type	Capacity	LUN
NETAPP iSCSI Disk (naa.60a9800...	Non-SSD	100,00 GB	11

Location
/vmfs/devices/disks/naa.60a98000324665714a5d426941774c58

Partition Format
GPT

Primary Partitions	Capacity
VMFS (NETAPP iSCSI Disk (naa.60a...	100,00 GB

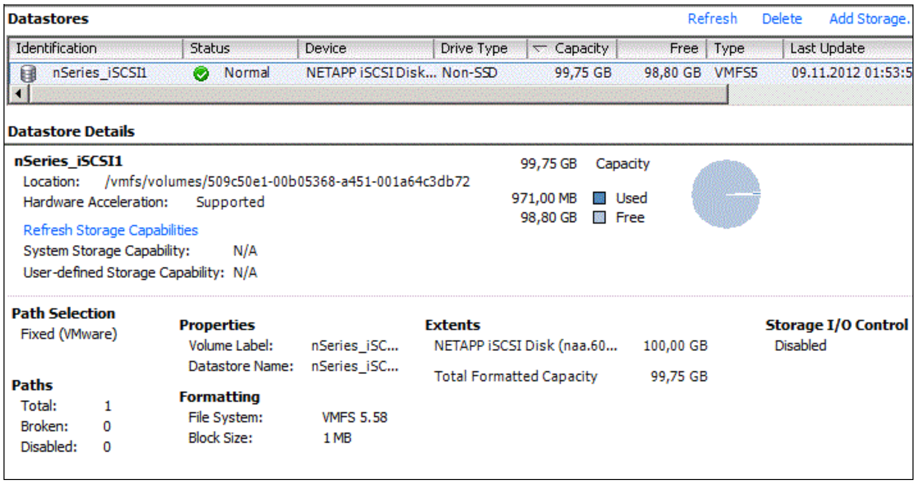
File system:

Properties
Datastore name: nSeries_iSCSI1

Formatting
File system: vmfs-5
Block size: 1 MB
Maximum file size: 2,00 TB

Figure 7-54 Reviewing datastore information

15. After the successful creation of the datastore, its information can be checked by clicking it (Figure 7-55), showing the number of paths, extents, block size, and path selection plug-in (PSP) being used.



Datastores Refresh Delete Add Storage.

Identification	Status	Device	Drive Type	Capacity	Free	Type	Last Update
nSeries_iSCSI1	✓ Normal	NETAPP iSCSI Disk...	Non-SSD	99,75 GB	98,80 GB	VMFS5	09.11.2012 01:53:5

Datastore Details

nSeries_iSCSI1
Location: /vmfs/volumes/509c50e1-00b05368-a451-001a64c3db72
Hardware Acceleration: Supported

99,75 GB Capacity
971,00 MB ■ Used
98,80 GB □ Free

Refresh Storage Capabilities
System Storage Capability: N/A
User-defined Storage Capability: N/A

Path Selection
Fixed (VMware)

Paths
Total: 1
Broken: 0
Disabled: 0

Properties
Volume Label: nSeries_iSC...
Datastore Name: nSeries_iSC...

Formatting
File System: VMFS 5.58
Block Size: 1 MB

Extents
NETAPP iSCSI Disk (naa.60... 100,00 GB
Total Formatted Capacity 99,75 GB

Storage I/O Control
Disabled

Figure 7-55 Reviewing datastore information

7.8 Creating a datastore cluster

Starting at vSphere 5, it is possible to create a cluster of storage in order to automatically distribute VMs among different datastores depending on its latency or free space available. This way, if a datastore free space falls below a specified limit, virtual disks can be automatically moved to another datastore undisruptivelly. This rearrangements are done by SDRS - Storage Distributed Resource Scheduler.

Even having those features enabled for all the datastores on that datastore cluster, specific VMs residing on them can be excluded from that process, enabling a granular control of the operations taking place.

To create a Storage cluster, perform the following steps:

1. Create at least two datastores using either SAN or NFS technologies.
2. On vSphere client, click **Home Inventory Datastores and Datastore Clusters**.
3. Right-click a cluster and select **New Datastore Cluster**, as shown in Figure 7-56.

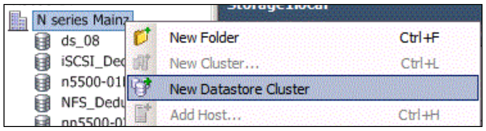
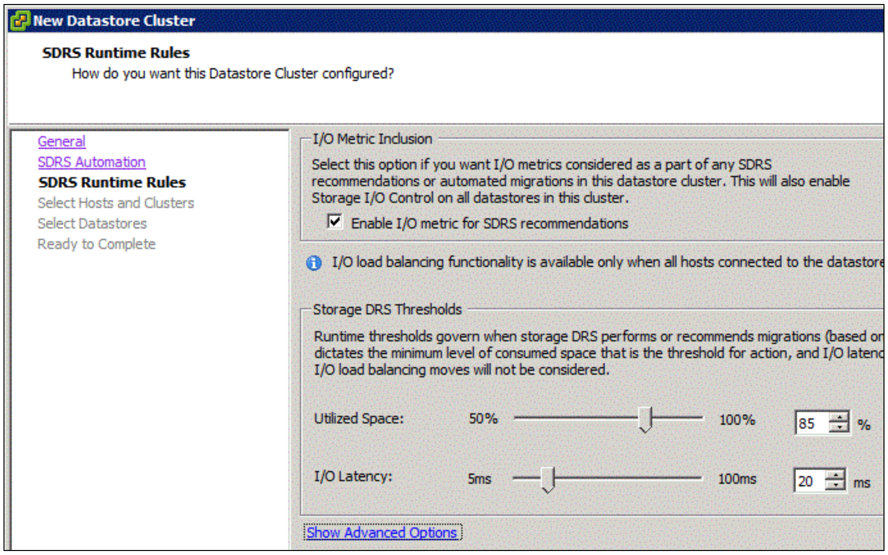


Figure 7-56 Creating a Datastore cluster

4. Type a name for that cluster and select **Turn on Storage DRS**, then click **Next**.
5. On Automation level window, select either **No automation** or **Fully automated** to determine how the moving of data will occur. No automation gives you more control over those operations, as you can review the recommendations before applying them, while Fully automated will executed them automatically. Click **Next** to set the thresholds for virtual disks move.
6. On SDRS Runtime Rules window, select Enable I/O metric for recommendations in order to allow the move of VM disk based on latency. Type the values determined as acceptable on your environment either for **Utilized space** and **I/O latency**, as shown in Figure 7-57, then click **Next**.



New Datastore Cluster

SDRS Runtime Rules

How do you want this Datastore Cluster configured?

I/O Metric Inclusion

Select this option if you want I/O metrics considered as a part of any SDRS recommendations or automated migrations in this datastore cluster. This will also enable Storage I/O Control on all datastores in this cluster.

☑ Enable I/O metric for SDRS recommendations

I/O load balancing functionality is available only when all hosts connected to the datastore

Storage DRS Thresholds

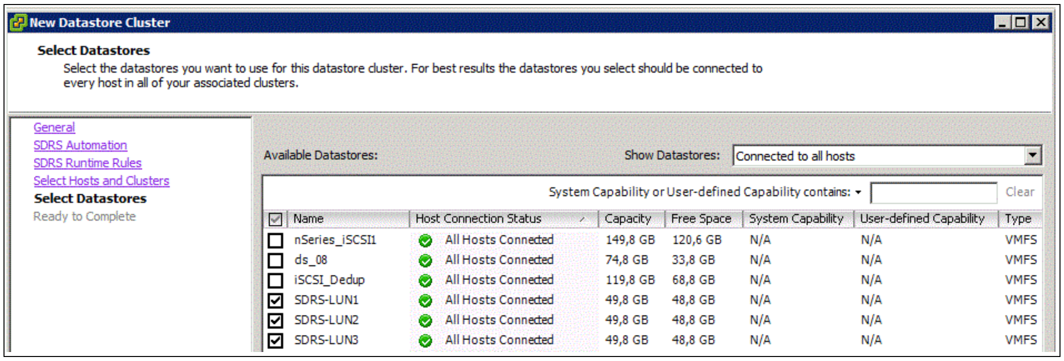
Runtime thresholds govern when storage DRS performs or recommends migrations (based or dictates the minimum level of consumed space that is the threshold for action, and I/O latenc I/O load balancing moves will not be considered.

Utilized Space: 50% 100% 85 %

I/O Latency: 5ms 100ms 20 ms

Figure 7-57 Defining the thresholds that trigger storage vMotion of VM disks

7. Select Hosts and Clusters window, select what of those elements will participate on the cluster, then click **Next**.
8. On the Select datastores window, select the previously created datastores that will belong to this cluster, as shown in Figure 7-58, and click **Next**.



New Datastore Cluster

Select Datastores

Select the datastores you want to use for this datastore cluster. For best results the datastores you select should be connected to every host in all of your associated clusters.

Available Datastores:

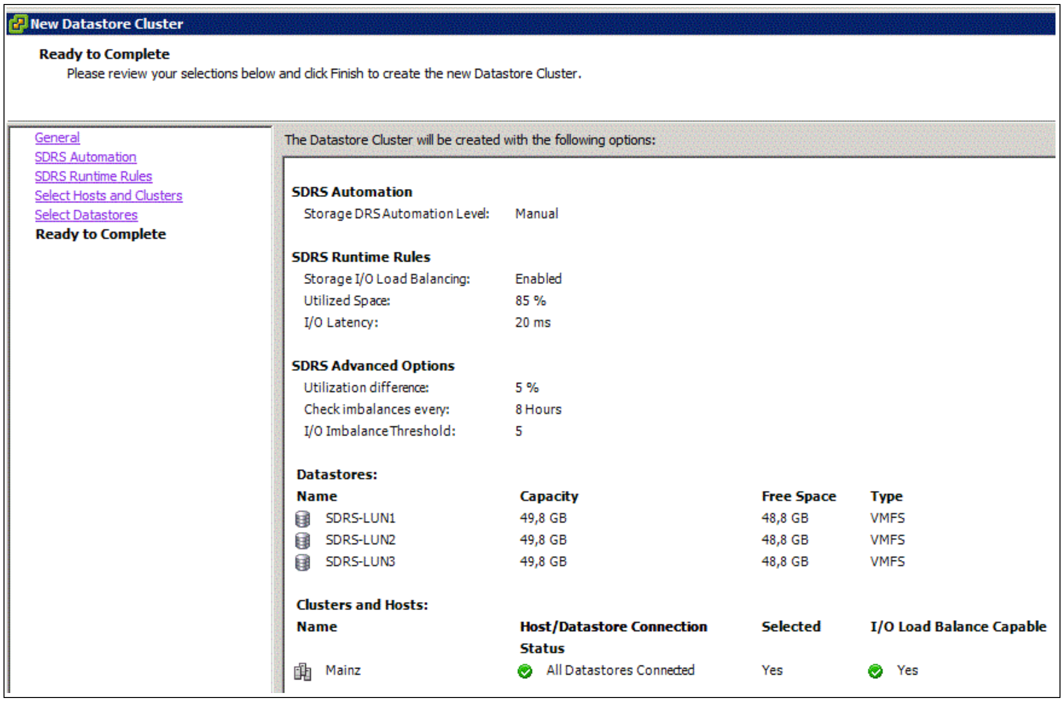
Show Datastores: Connected to all hosts

System Capability or User-defined Capability contains:

☑	Name	Host Connection Status	Capacity	Free Space	System Capability	User-defined Capability	Type
□	nSeries_iSCSI1	All Hosts Connected	149,8 GB	120,6 GB	N/A	N/A	VMFS
□	ds_08	All Hosts Connected	74,8 GB	33,8 GB	N/A	N/A	VMFS
□	iSCSI_Dedup	All Hosts Connected	119,8 GB	68,8 GB	N/A	N/A	VMFS
☑	SDRS-LUN1	All Hosts Connected	49,8 GB	48,8 GB	N/A	N/A	VMFS
☑	SDRS-LUN2	All Hosts Connected	49,8 GB	48,8 GB	N/A	N/A	VMFS
☑	SDRS-LUN3	All Hosts Connected	49,8 GB	48,8 GB	N/A	N/A	VMFS

Figure 7-58 Selecting the datastore participating on the storage cluster

9. Check the information previously entered, as shown in Figure 7-59, and click **Finish**.



Ready to Complete

Please review your selections below and click Finish to create the new Datastore Cluster.

The Datastore Cluster will be created with the following options:

SDRS Automation

Storage DRS Automation Level:	Manual

SDRS Runtime Rules

Storage I/O Load Balancing:	Enabled
Utilized Space:	85 %
I/O Latency:	20 ms

SDRS Advanced Options

Utilization difference:	5 %
Check imbalances every:	8 Hours
I/O Imbalance Threshold:	5

Datastores:

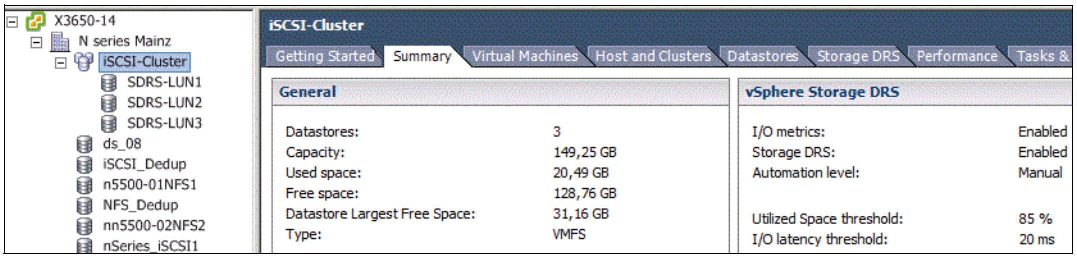
Name	Capacity	Free Space	Type
SDRS-LUN1	49,8 GB	48,8 GB	VMFS
SDRS-LUN2	49,8 GB	48,8 GB	VMFS
SDRS-LUN3	49,8 GB	48,8 GB	VMFS

Clusters and Hosts:

Name	Host/Datastore Connection Status	Selected	I/O Load Balance Capable
Mainz	✓ All Datastores Connected	Yes	✓ Yes

Figure 7-59 Reviewing datastore cluster information

A datastore cluster looks like Figure 7-60.



General

Datastores:	3
Capacity:	149,25 GB
Used space:	20,49 GB
Free space:	128,76 GB
Datastore Largest Free Space:	31,16 GB
Type:	VMFS

vSphere Storage DRS

I/O metrics:	Enabled
Storage DRS:	Enabled
Automation level:	Manual
Utilized Space threshold:	85 %
I/O latency threshold:	20 ms

Figure 7-60 A datastore cluster

7.9 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:

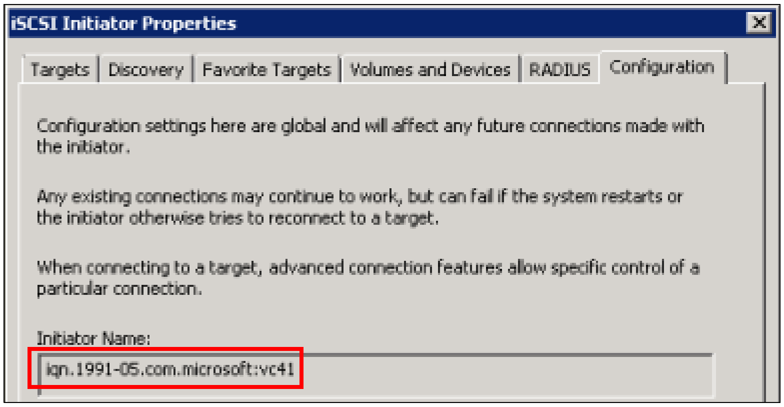
1. On Windows 2008, click **Start** → **Administrative Tools** → **iSCSI Initiator**. On Windows 2003, the iSCSI client must be downloaded from the following website:

   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 7-61. If you want to change it, click the **Change** button and make your modifications accordingly.



Configuration settings here are global and will affect any future connections made with the initiator.

Any existing connections may continue to work, but can fail if the system restarts or the initiator otherwise tries to reconnect to a target.

When connecting to a target, advanced connection features allow specific control of a particular connection.

Initiator Name:

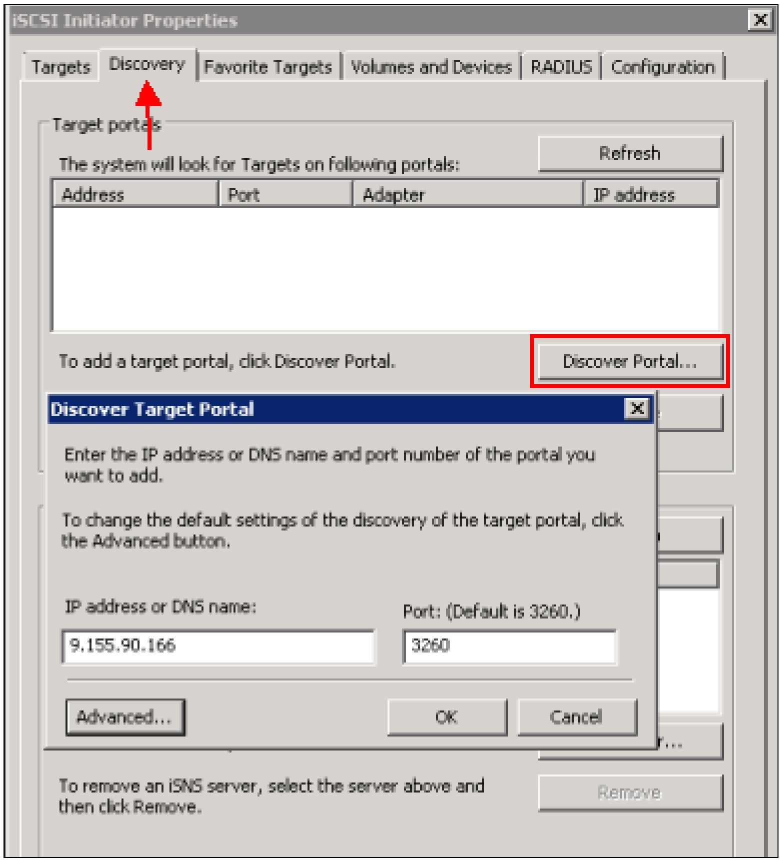
iqn.1991-05.com.microsoft:vc41

Figure 7-61 Collecting the VM's IQN

4. Create an iSCSI Initiator group, as described in 7.3.3, “Creating an initiator group on N series systems” on page 106.

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 7-62.



Target portals

The system will look for Targets on following portals:

To add a target portal, click Discover Portal.

Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

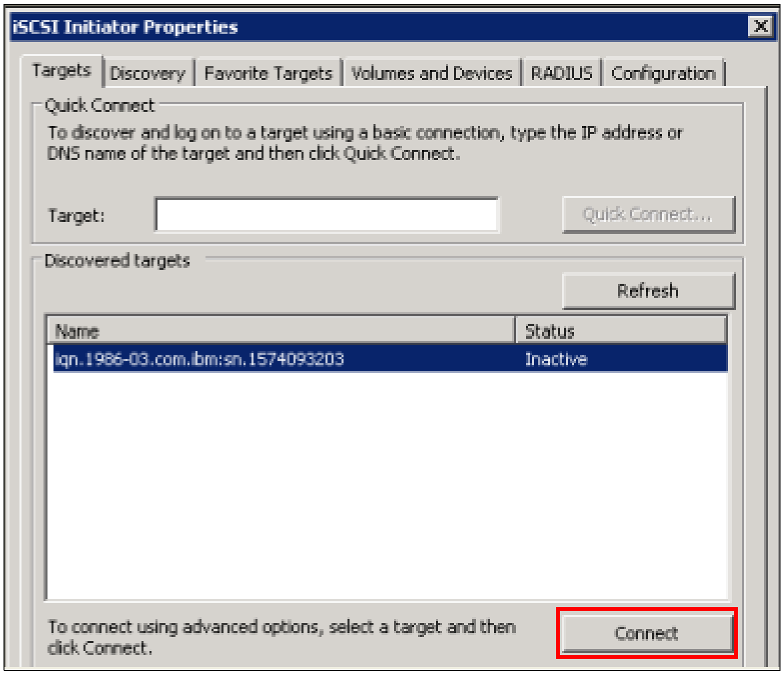
IP address or DNS name: 9.155.90.166

Port: (Default is 3260.) 3260

To remove an iSNS server, select the server above and then click Remove.

Figure 7-62 Adding the storage iSCSI data interface

7. Click **Targets**; the N series IQN will display as Inactive. Click **Connect**, as shown in Figure 7-63.



Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

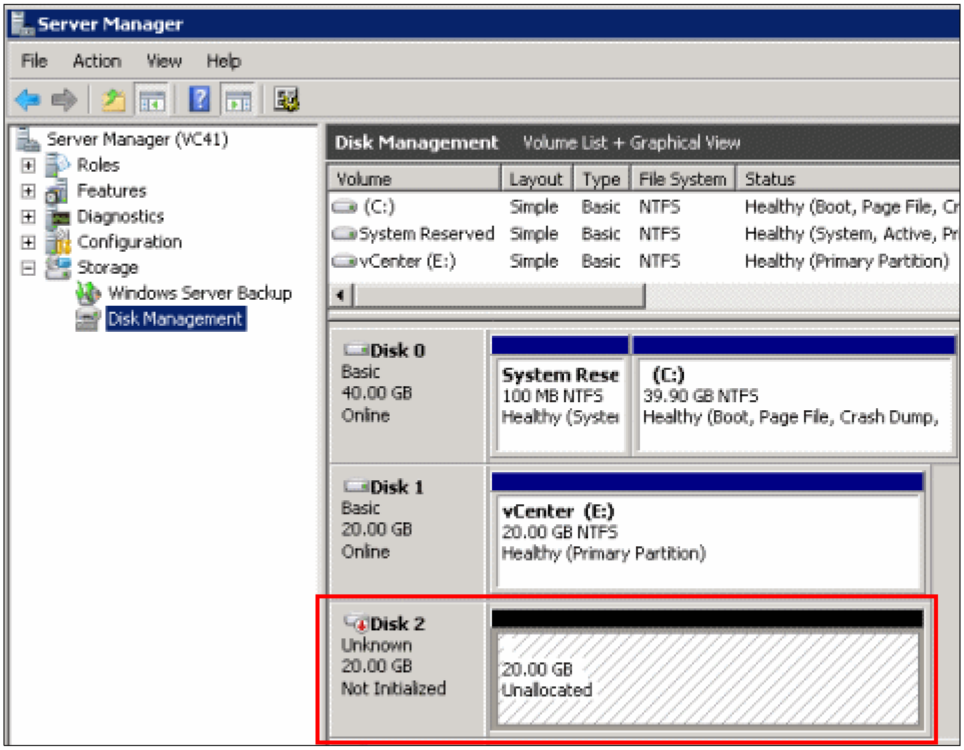
Discovered targets

Name	Status
iqn.1986-03.com.ibm:sn.1574093203	Inactive

To connect using advanced options, select a target and then click Connect.

Figure 7-63 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 shown in Figure 7-64. If not, right-click **Disk Management** and select **Rescan**.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Cr
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Pr
vCenter (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)

Disk 0
Basic
40.00 GB
Online

System Rese
100 MB NTFS
Healthy (Syste

(C:)
39.90 GB NTFS
Healthy (Boot, Page File, Crash Dump,

Disk 1
Basic
20.00 GB
Online

vCenter (E:)
20.00 GB NTFS
Healthy (Primary Partition)

Disk 2
Unknown
20.00 GB
Not Initialized

20.00 GB
Unallocated

Figure 7-64 The allocated LUN shows in Disk Management

7.10 NFS volumes on VMware vSphere 5.1

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, reflecting those operations on the VMware side with a rescan of its storage adapters.

NFS also offers an advantage of the datastore size that can be created. The VMware host does not have a limit for it, so the datastore can be as large as the storage volume size supported by the storage, which currently is 100 TB. It gives the administrator a central management point, instead of managing multiple datastores as with VMFS datastores.

Also, the integration on NFS and N series provides transparent access to VM-level storage virtualization offerings such as production-use block-level data deduplication, immediate zero-cost VM and datastore clones, array-based thin provisioning, automated policy-based datastore resizing, and direct access to array-based Snapshot copies.

Using NFS is also supported with integrated tools such as the Site Recovery Adapter for Site Recovery Manager and the VSC.

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.

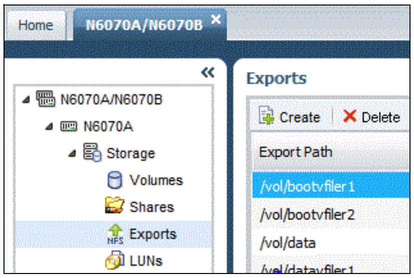
VMware hosts require the creation of a VMkernel portgroup in order to access NFS. It is necessary because all the traffic between the storage system and the host must flow through IP network.

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

7.10.1 Setting up an NFS volume on N series

To create an NFS export, perform the following steps:

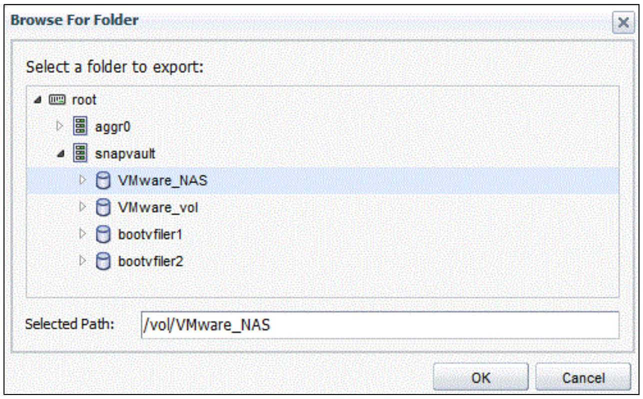
1. Expand the storage where the NFS export will reside, and then click **Exports**, and then **Create**, as shown in Figure 7-65.



Export Path
/vol/bootvfiler1
/vol/bootvfiler2
/vol/data
/vol/datavfiler1

Figure 7-65 Navigating to NFS Exports

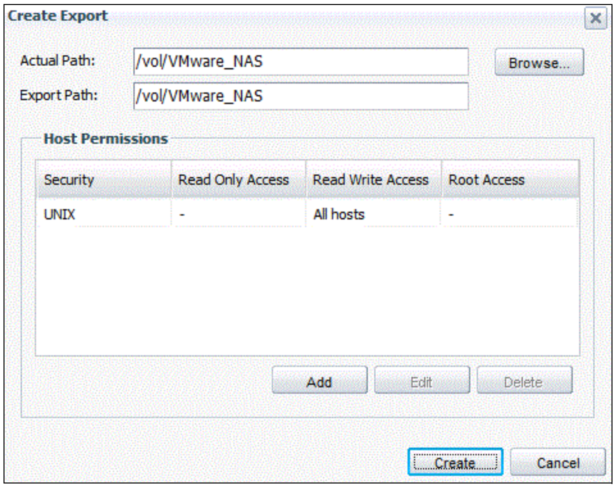
2. Create Export: Click **Browse** to select the existing volume where the NFS will be stored, then add a name for the NFS export, as shown in Figure 7-66, and click **OK**.



Selected Path: /vol/VMware_NAS

Figure 7-66 Selecting the volume to hold the NFS export

3. Add the NFS export name after the volume name, then select the entry on Host Permissions and click **Edit**, as shown in Figure 7-67.



Actual Path: /vol/VMware_NAS

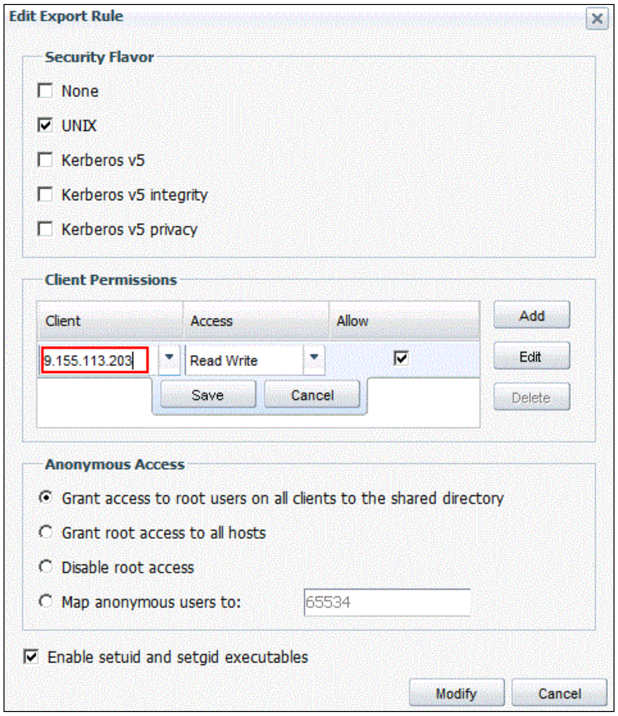
Export Path: /vol/VMware_NAS

Host Permissions

Security	Read Only Access	Read Write Access	Root Access
UNIX	-	All hosts	-

Figure 7-67 Adding NFS export name and editing Host Permissions

4. Select the Client Permissions entry and click **Edit**, then replace the original entry All Clients by the IP of the servers that will access that export (Figure 7-68). Click **Save**, then click **Add** and repeat the process for all the hosts as needed, then click **Modify**.



Security Flavor

☐ None

☑ UNIX

☐ Kerberos v5

☐ Kerberos v5 integrity

☐ Kerberos v5 privacy

Client Permissions

Client	Access	Allow
9.155.113.203	Read Write	☑

Anonymous Access

● Grant access to root users on all clients to the shared directory

○ Grant root access to all hosts

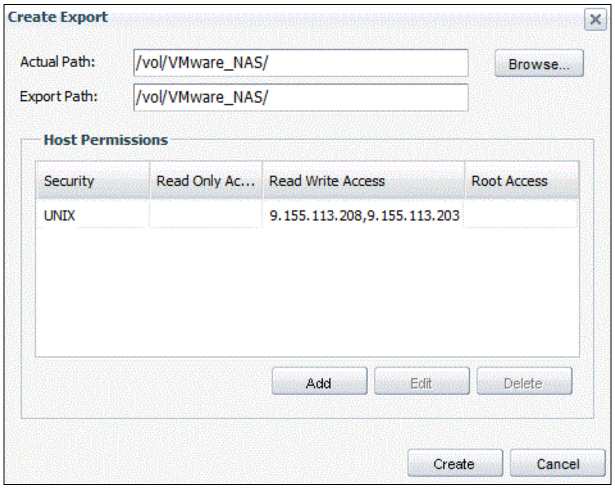
○ Disable root access

○ Map anonymous users to: 65534

☑ Enable setuid and setgid executables

Figure 7-68 Changing Client Permissions

5. The final window should look like Figure 7-69. Click **Create** to complete.



Actual Path: /vol/VMware_NAS/

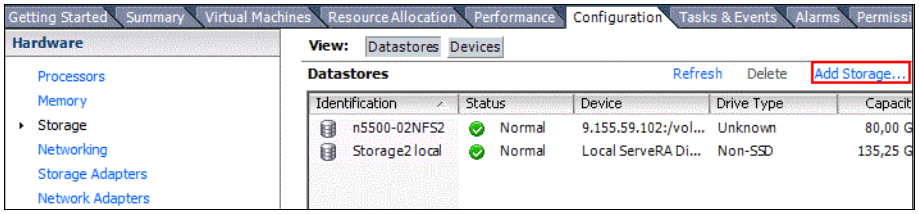
Export Path: /vol/VMware_NAS/

Host Permissions

Security	Read Only Ac...	Read Write Access	Root Access
UNIX		9.155.113.208,9.155.113.203	

Figure 7-69 NFS export and servers with access to it

6. From the vSphere Client, navigate to the window shown in Figure 7-70.



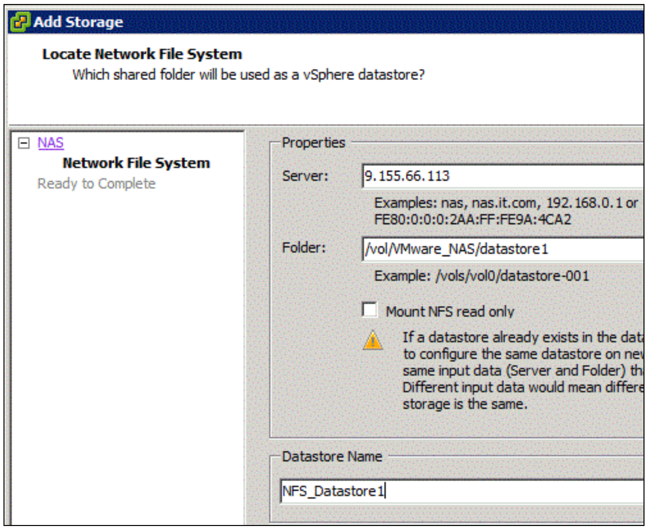
Datastores

Identification	Status	Device	Drive Type	Capacit
n5500-02NFS2	Normal	9.155.59.102:/vol...	Unknown	80,00 G
Storage2 local	Normal	Local ServeRA Di...	Non-SSD	135,25 G

Figure 7-70 Adding storage

7. Select NFS, and click **Next**.

8. In the Locate Network File System panel (Figure 7-71), complete the steps shown.



Locate Network File System

Which shared folder will be used as a vSphere datastore?

Server: 9.155.66.113

Examples: nas, nas.it.com, 192.168.0.1 or FE80:0:0:0:2AA:FF:FE9A:4CA2

Folder: /vol/VMware_NAS/datastore1

Example: /vols/vol0/datastore-001

☐ Mount NFS read only

If a datastore already exists in the dat to configure the same datastore on ne same input data (Server and Folder) th Different input data would mean differe storage is the same.

Datastore Name: NFS_Datastore1

Figure 7-71 Define NFS export parameters

Here we summarize the required steps:

i. Enter the storage system and volume name so that the ESX host can locate it.

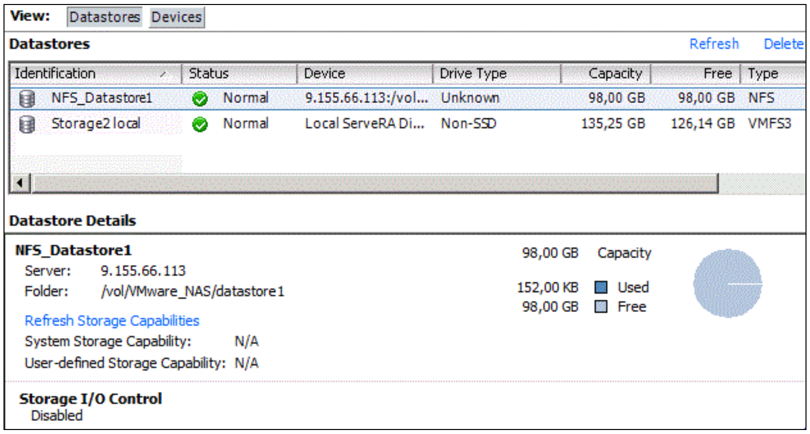
ii. Optional: Select **Mount NFS read only**, if your NFS volume is read only.

iii. In the field Datastore Name, enter the datastore name of that NFS volume.

iv. Click **Next**.

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

10. After the connection between the ESX host and the N series is established, the NFS volume is mounted, as shown in Figure 7-72.



Datastores

Identification	Status	Device	Drive Type	Capacity	Free	Type
NFS_Datastore1	Normal	9.155.66.113:/vol...	Unknown	98,00 GB	98,00 GB	NFS
Storage2 local	Normal	Local ServeRA Di...	Non-SSD	135,25 GB	126,14 GB	VMFS3

Datastore Details

NFS_Datastore1
Server: 9.155.66.113
Folder: /vol/VMware_NAS/datastore1

98,00 GB Capacity
152,00 KB ■ Used
98,00 GB □ Free

Refresh Storage Capabilities
System Storage Capability: N/A
User-defined Storage Capability: N/A

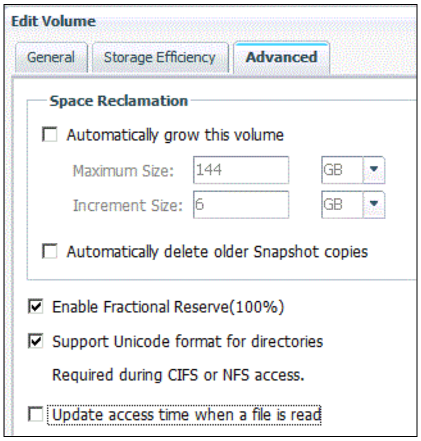
Storage I/O Control
Disabled

Figure 7-72 NFS datastore details

7.10.2 NFS datastore limits and options

By default, an ESXi 5 host is capable to connect to up to 256 NFS datastores. It is an expressive improvement compared to version vSphere version 4, where the maximum number of NFS datastores was 64.

When deploying VMDKs on NFS, disable the access time updates that occur by default on the NFS. To disable the access time updates, uncheck the option **Update access time when file is read** on the Advanced tab of the NFS volume, as shown in Figure 7-73.



Space Reclamation

□ Automatically grow this volume

Maximum Size: 144 GB

Increment Size: 6 GB

□ Automatically delete older Snapshot copies

☑ Enable Fractional Reserve(100%)

☑ Support Unicode format for directories

Required during CIFS or NFS access.

□ Update access time when a file is read

Figure 7-73 Disabling Update access time

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:

http://www.redbooks.ibm.com/abstracts/sg247734.html?Open

7.12 Storage growth management

This section explains how to grow different storage types used to house virtual machines.

7.12.1 Growing VMFS datastores

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 IBM N series System Manager:

   `http://Nseries/na_admin`

2. Navigate to your storage device, select **Storage** → **LUNs**, then right-click the desired LUN and click **Edit**, as shown in Figure 7-74.

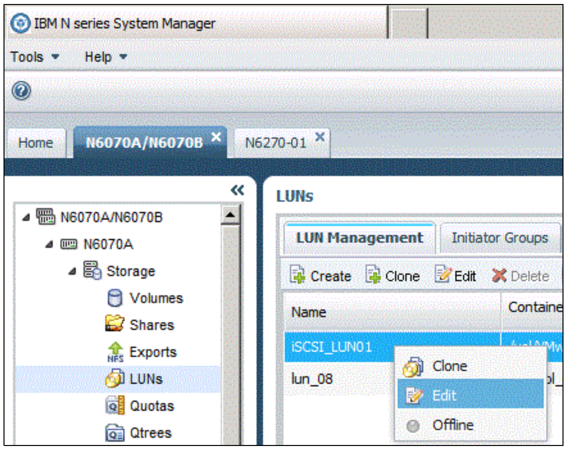
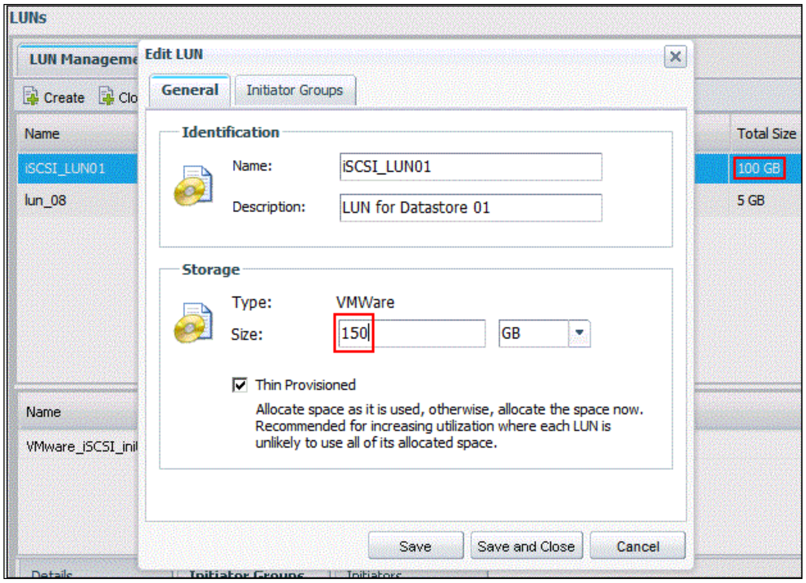


Figure 7-74 Editing the LUN

3. On Edit LUN window, type the new size of that LUN, as shown in Figure 7-75. You can see the current size on the right on Total Size (100 GB) while the new LUN size will be 150 GB. Click **Save and Close**.



Name: iSCSI_LUN01

Description: LUN for Datastore 01

Type: VMWare

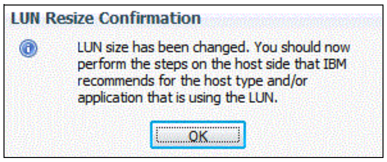
Size: 150 GB

☑ Thin Provisioned

Allocate space as it is used, otherwise, allocate the space now. Recommended for increasing utilization where each LUN is unlikely to use all of its allocated space.

Figure 7-75 Growing a LUN

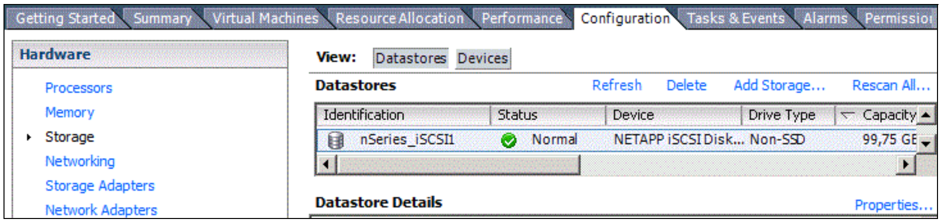
4. Click **OK** on the message stating that the LUN is Thin Provisioned and thus the space might not be actually added if there is no space on the volume holding it.
5. A message will display showing that the resize was completed successfully (Figure 7-76).



LUN size has been changed. You should now perform the steps on the host side that IBM recommends for the host type and/or application that is using the LUN.

Figure 7-76 LUN extended successfully

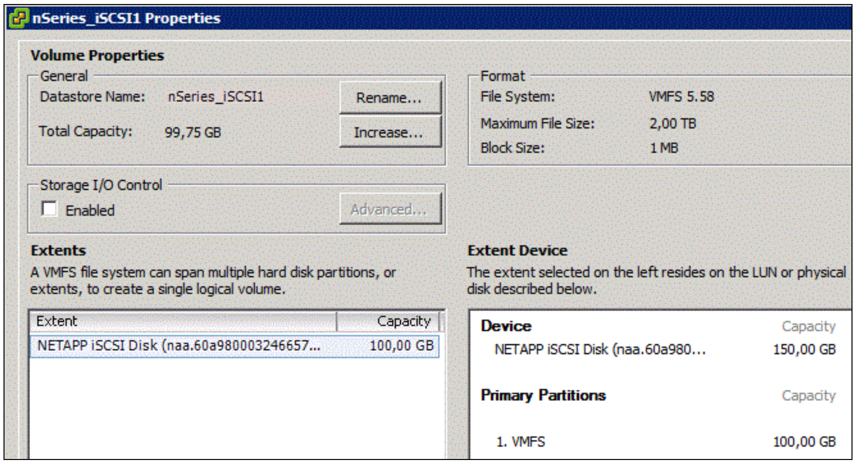
6. Return to VMware Infrastructure Client and select a host connected to that LUN. Then go to the Configuration tab, then select Storage in the left, then click **Rescan Adapters**.
7. After the rescan completion, click the datastore to be expanded and click **Properties**, as shown in Figure 7-77.



Identification	Status	Device	Drive Type	Capacity
nSeries_iSCSI1	Normal	NETAPP iSCSI Disk...	Non-SSD	99,75 GE

Figure 7-77 Clicking Properties of the datastore to be expanded

8. The new LUN size will be displayed on the datastore properties, as shown in Capacity Device in Figure 7-78. Click **Increase** to extend the datastore.



nSeries_iSCSI1 Properties

Volume Properties

General

Datastore Name: nSeries_iSCSI1 Rename...

Total Capacity: 99,75 GB Increase...

Format

File System: VMFS 5.58

Maximum File Size: 2,00 TB

Block Size: 1 MB

Storage I/O Control

☐ Enabled Advanced...

Extents

A VMFS file system can span multiple hard disk partitions, or extents, to create a single logical volume.

Extent	Capacity
NETAPP iSCSI Disk (naa.60a980003246657...	100,00 GB

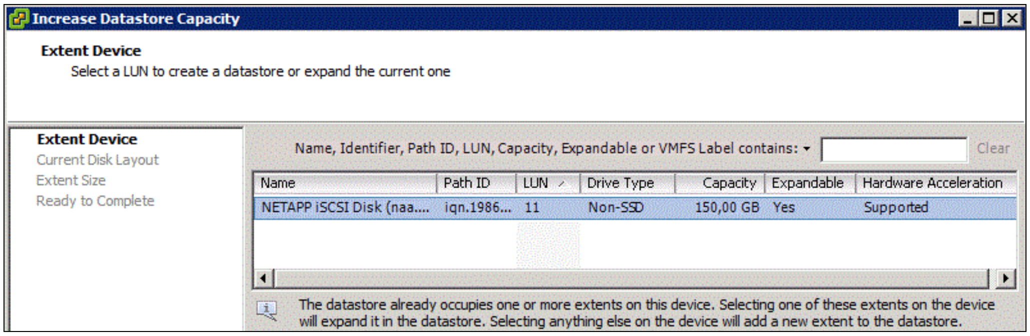
Extent Device

The extent selected on the left resides on the LUN or physical disk described below.

Device	Capacity
NETAPP iSCSI Disk (naa.60a980...	150,00 GB
Primary Partitions	Capacity
1. VMFS	100,00 GB

Figure 7-78 The new LUN size (150 GB) is shown

9. Notice that the same LUN has additional 50 GB and is marked as expandable, as shown in Figure 7-79. Click **Next**.



Increase Datastore Capacity

Extent Device

Select a LUN to create a datastore or expand the current one

Extent Device
Current Disk Layout
Extent Size
Ready to Complete

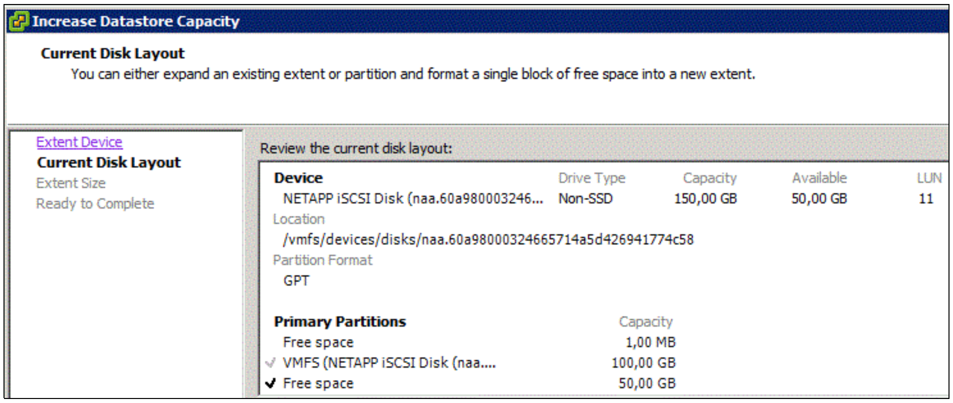
Name, Identifier, Path ID, LUN, Capacity, Expandable or VMFS Label contains: ▾ Clear

Name	Path ID	LUN	Drive Type	Capacity	Expandable	Hardware Acceleration
NETAPP iSCSI Disk (naa....	iqn.1986...	11	Non-SSD	150,00 GB	Yes	Supported

The datastore already occupies one or more extents on this device. Selecting one of these extents on the device will expand it in the datastore. Selecting anything else on the device will add a new extent to the datastore.

Figure 7-79 LUN with additional space

10. The same information is shown more explicitly on the next window (Figure 7-80).



Increase Datastore Capacity

Current Disk Layout

You can either expand an existing extent or partition and format a single block of free space into a new extent.

Extent Device
Current Disk Layout
Extent Size
Ready to Complete

Review the current disk layout:

Device	Drive Type	Capacity	Available	LUN
NETAPP iSCSI Disk (naa.60a980003246...	Non-SSD	150,00 GB	50,00 GB	11

Location

/vmfs/devices/disks/naa.60a98000324665714a5d426941774c58

Partition Format

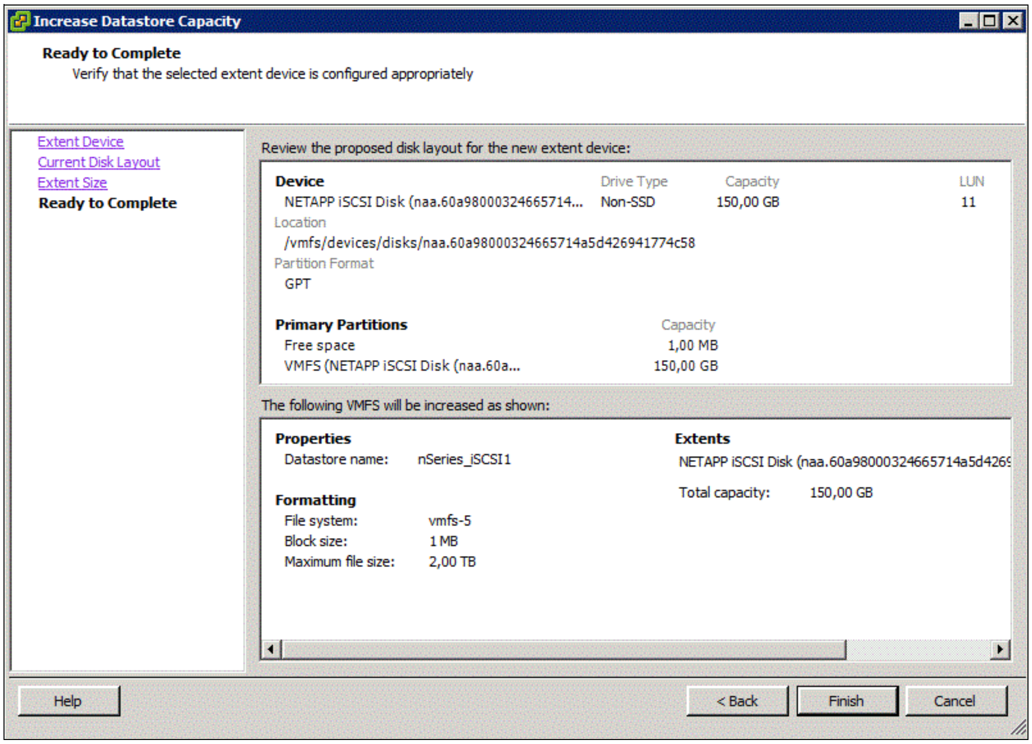
GPT

Primary Partitions	Capacity
Free space	1,00 MB
✓ VMFS (NETAPP iSCSI Disk (naa....	100,00 GB
✓ Free space	50,00 GB

Figure 7-80 The current space being used and the space available to increase the datastore

11. Select how much space to add to the datastore and click **Next**.

12. Review the details of the growth and click **Finish**, as shown in Figure 7-81.



Ready to Complete
Verify that the selected extent device is configured appropriately

Review the proposed disk layout for the new extent device:

Device	Drive Type	Capacity	LUN
NETAPP iSCSI Disk (naa.60a98000324665714...	Non-SSD	150,00 GB	11

Location
/vmfs/devices/disks/naa.60a98000324665714a5d426941774c58

Partition Format
GPT

Primary Partitions	Capacity
Free space	1,00 MB
VMFS (NETAPP iSCSI Disk (naa.60a...	150,00 GB

The following VMFS will be increased as shown:

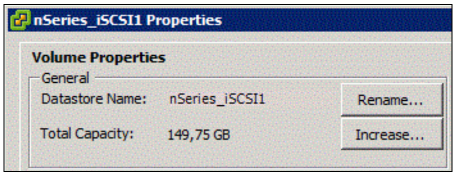
Properties
Datastore name: nSeries_iSCSI1

Extents
NETAPP iSCSI Disk (naa.60a98000324665714a5d426
Total capacity: 150,00 GB

Formatting
File system: vmfs-5
Block size: 1 MB
Maximum file size: 2,00 TB

Figure 7-81 Review the expansion details

13. The next window shows the datastore expanded after that operation, as shown in Figure 7-82.



Volume Properties
General
Datastore Name: nSeries_iSCSI1
Total Capacity: 149,75 GB

Figure 7-82 Datastore with its new capacity

7.12.2 Growing an NFS datastore

To grow an NFS datastore, it is only necessary to grow the NFS volume and rescan the host, performing the following steps:

1. Open IBM N series System Manager, navigate to the volume that needs to be expanded, right-click it, and select **Resize**, as shown in Figure 7-83.

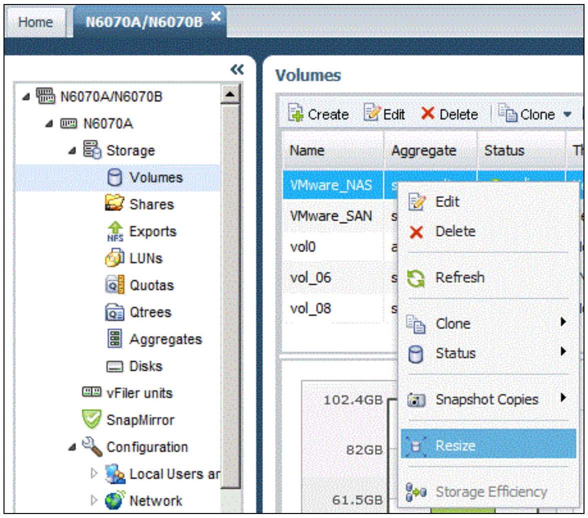
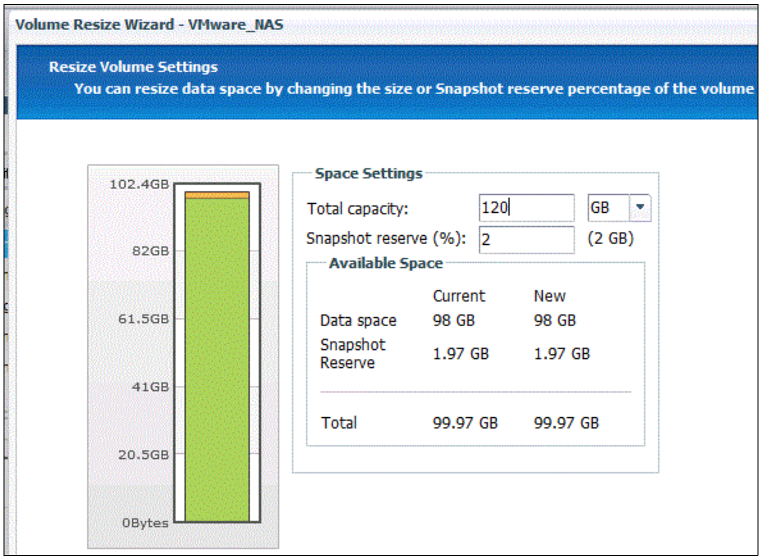


Figure 7-83 Resizing a volume

2. On the Welcome to the Volume Resize Wizard window, click **Next**.
3. Type the new volume size (our example grows from 100 GB to 120 GB) as shown in Figure 7-84 and click **Next**.


Volume Resize Wizard - VMware_NAS

Resize Volume Settings

You can resize data space by changing the size or Snapshot reserve percentage of the volume

Space Settings

Total capacity: 120 GB

Snapshot reserve (%): 2 (2 GB)

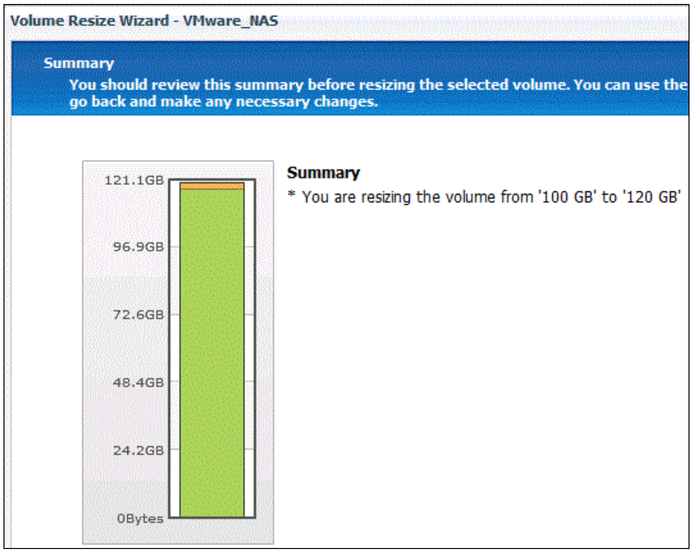
Available Space

	Current	New
Data space	98 GB	98 GB
Snapshot Reserve	1.97 GB	1.97 GB
Total	99.97 GB	99.97 GB

Figure 7-84 Type new volume size

4. Click **Next** on the Select Snapshots to be Deleted or select Snapshots that you might want to delete, but be aware that it might affect your ability to recover files saved on those Snapshots.

5. Review the volume growth information as shown in Figure 7-85 and click **Next**.



Volume Resize Wizard - VMware_NAS

Summary

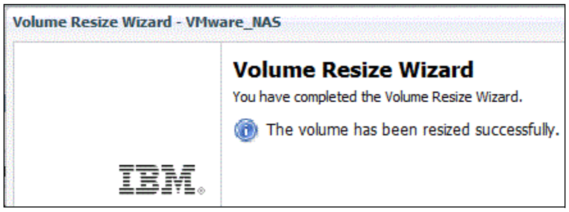
You should review this summary before resizing the selected volume. You can use the go back and make any necessary changes.

Summary

* You are resizing the volume from '100 GB' to '120 GB'

Figure 7-85 Summary of changes being made to the volume

6. If the growth completed successfully, a success message will be shown (see Figure 7-86). Then click **Finish** to complete the process.



Volume Resize Wizard - VMware_NAS

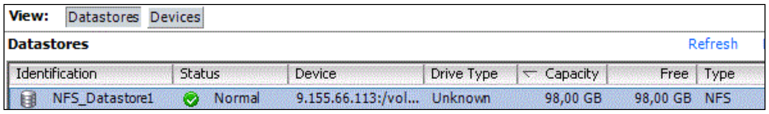
Volume Resize Wizard

You have completed the Volume Resize Wizard.

The volume has been resized successfully.

Figure 7-86 A successful growth of volume

7. Going back to vSphere client, select one the hosts connected to that NFS datastore and check its space, as shown in Figure 7-87.



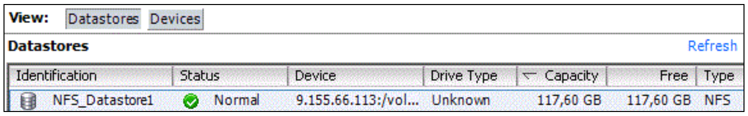
View: Datastores Devices

Datastores Refresh

Identification	Status	Device	Drive Type	Capacity	Free	Type
NFS_Datastore1	Normal	9.155.66.113:/vol...	Unknown	98,00 GB	98,00 GB	NFS

Figure 7-87 The NFS datastore size before the rescan

8. Run a **Rescan All...** and check details for that datastore again (Figure 7-88).



View: Datastores Devices

Datastores Refresh

Identification	Status	Device	Drive Type	Capacity	Free	Type
NFS_Datastore1	Normal	9.155.66.113:/vol...	Unknown	117,60 GB	117,60 GB	NFS

Figure 7-88 The NFS datastore size after the rescan

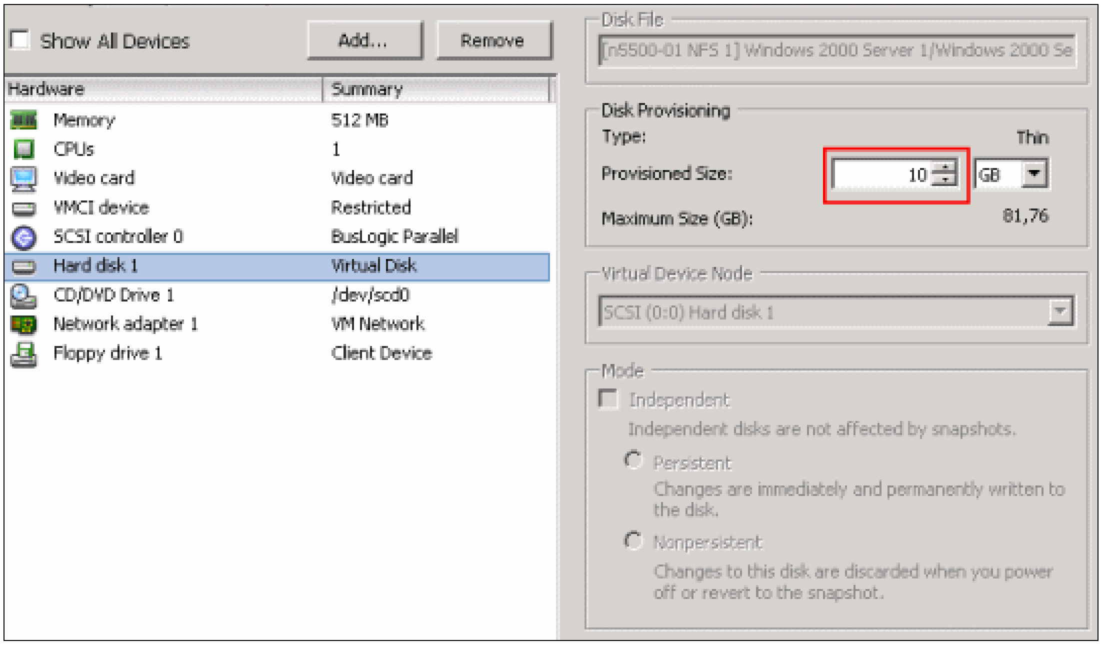
7.12.3 Growing a virtual disk

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 141.

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 7-89. Then click **OK**.



□ Show All Devices

Hardware	Summary
Memory	512 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	BusLogic Parallel
Hard disk 1	Virtual Disk
CD/DVD Drive 1	/dev/scd0
Network adapter 1	VM Network
Floppy drive 1	Client Device

Disk File

[n5500-01 NFS 1] Windows 2000 Server 1/Windows 2000 Se

Disk Provisioning

Type: Thin

Provisioned Size: 10 GB

Maximum Size (GB): 81,76

Virtual Device Node

SCSI (0:0) Hard disk 1

Mode

□ Independent

Independent disks are not affected by snapshots.

○ Persistent

Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

Figure 7-89 Growing a virtual disk

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. Connect to the guest.
2. Grow the file system.
   a. Windows 2008 can use the graphical interface to extend the disks, using Disk Management.

b. For Windows 2000 and Windows 2003 guests, 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

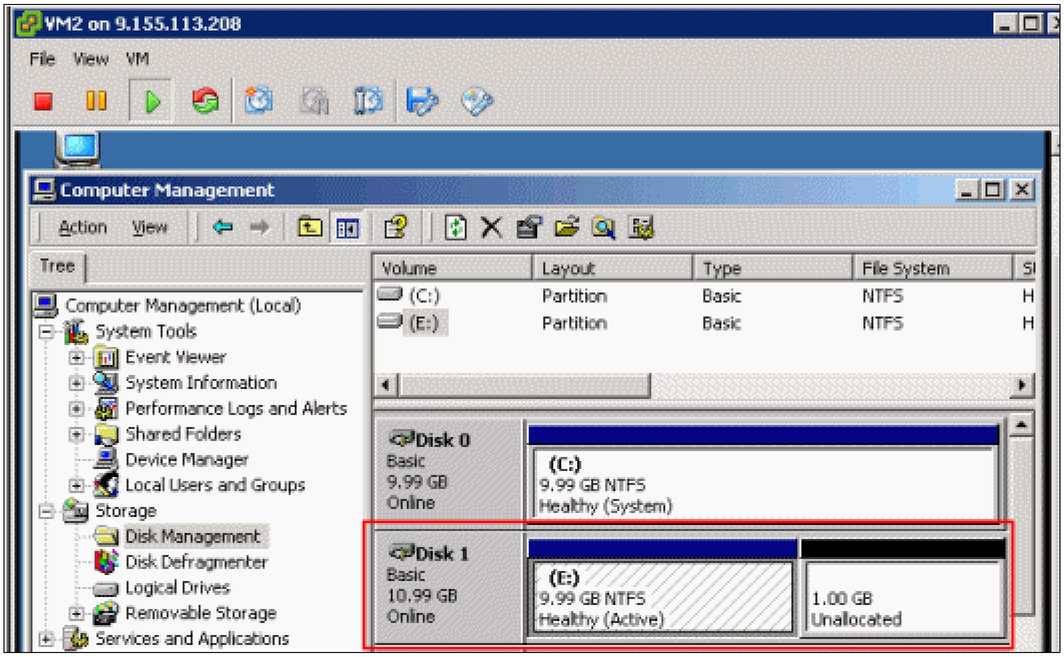
c. For Linux guests, use **ext2resize** to grow a file system. For more information, see the following web page from SourceForge:

http://sourceforge.net/projects/ext2resize

Growing bootable volumes

Root volumes, such as C:\ in Windows guests running Windows 2000 and Windows 2003, or / in Linux guests, cannot be grown while the guest is running. However, they can be expanded if they are not running as a boot volume, by attaching it to another VM running same operating system type, and then following a common disk expansion processes defined in “Growing a virtual disk” on page 140. The following example explains how to perform that operation on a Windows 2003 server:

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 (Figure 7-90).



Volume	Layout	Type	File System	St
(C:)	Partition	Basic	NTFS	H
(E:)	Partition	Basic	NTFS	H

Disk 0
Basic
9.99 GB
Online

(C:)
9.99 GB NTFS
Healthy (System)

Disk 1
Basic
10.99 GB
Online

(E:)
9.99 GB NTFS
Healthy (Active)

1.00 GB
Unallocated

Figure 7-90 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 re-add 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 5.1. It includes the following topics:

- VMware and N series cloning technologies
- Cloning guests within a datastore
- Cloning an entire datastore
- Cloning VMware ESXi servers

© Copyright IBM Corp. 2013. All rights reserved.

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.

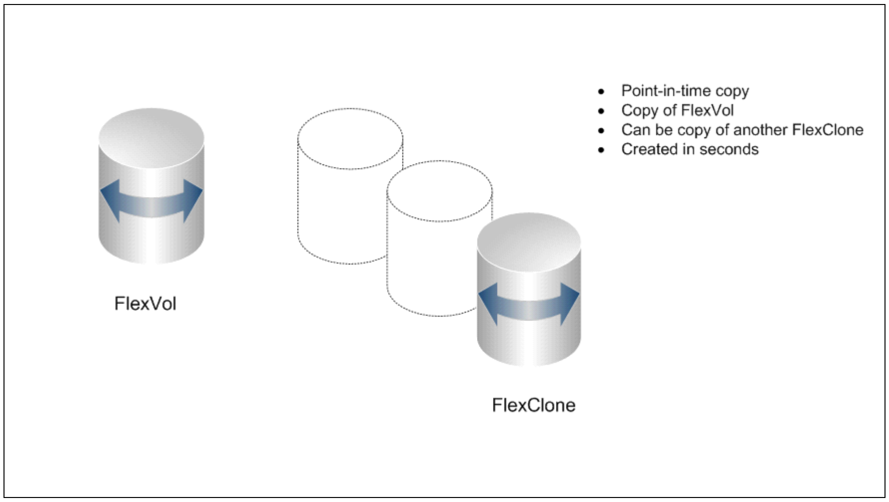


Figure 8-1 FlexClone

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.

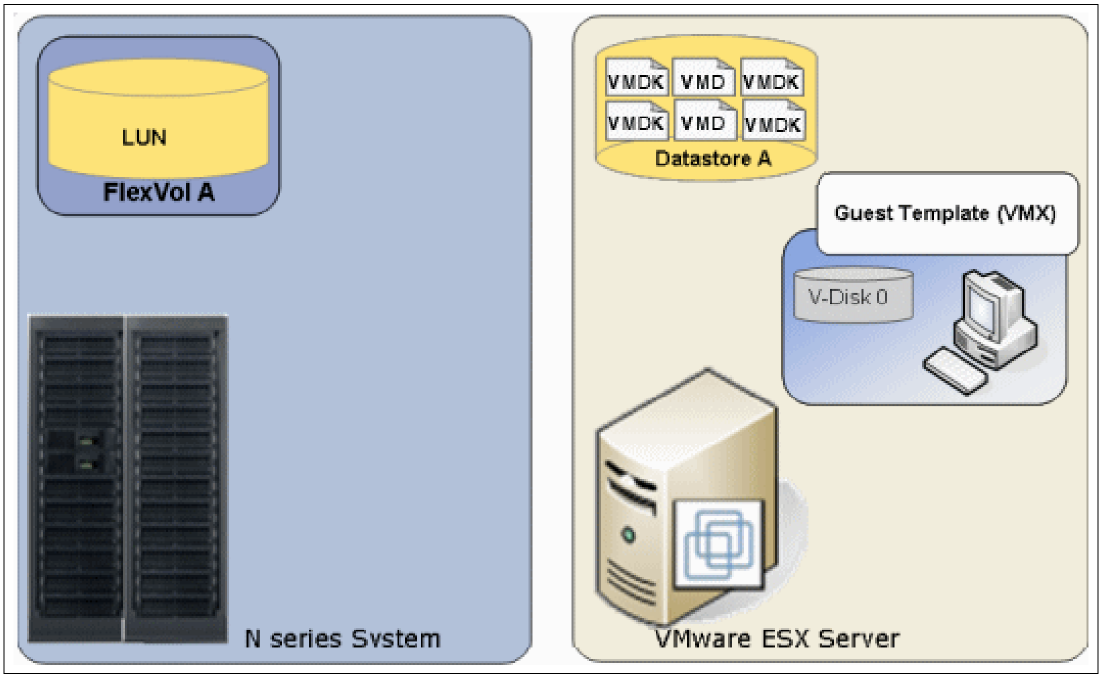


Figure 8-2 A datastore with six cloned guests

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.

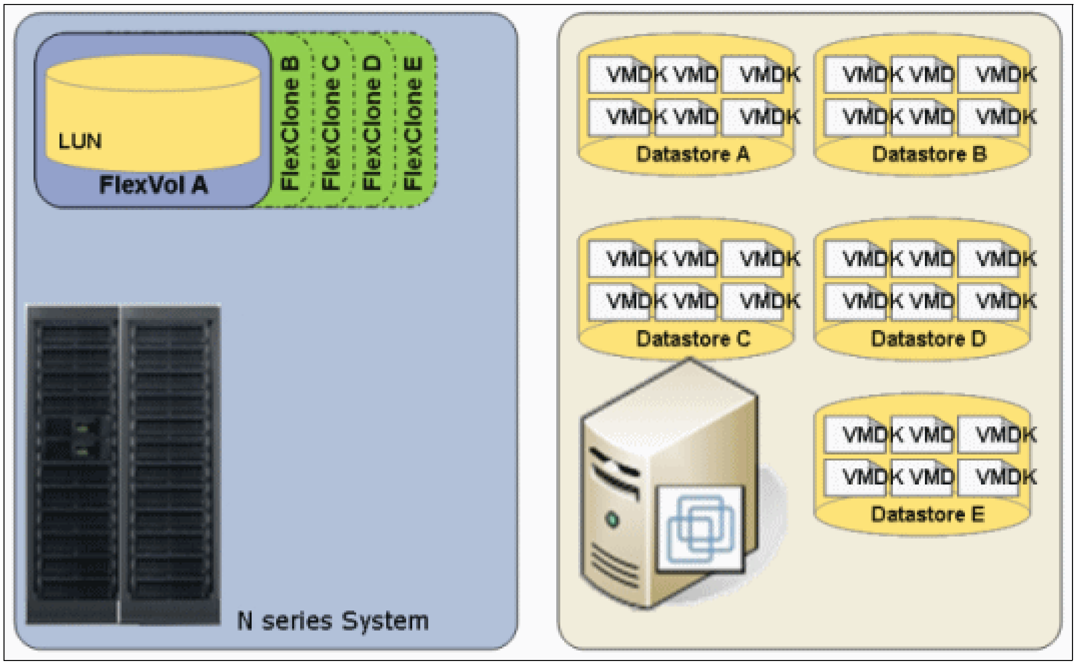


Figure 8-3 Virtual infrastructure with four quickly deployed, space-efficient datastores

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**.

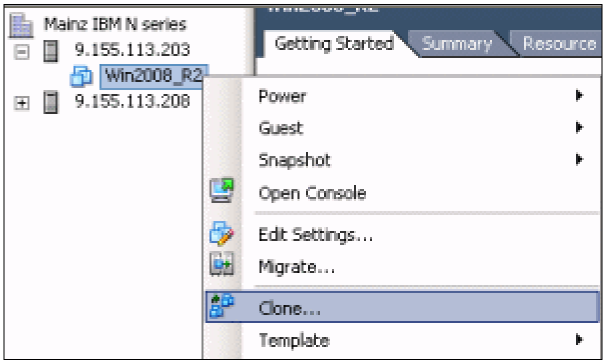
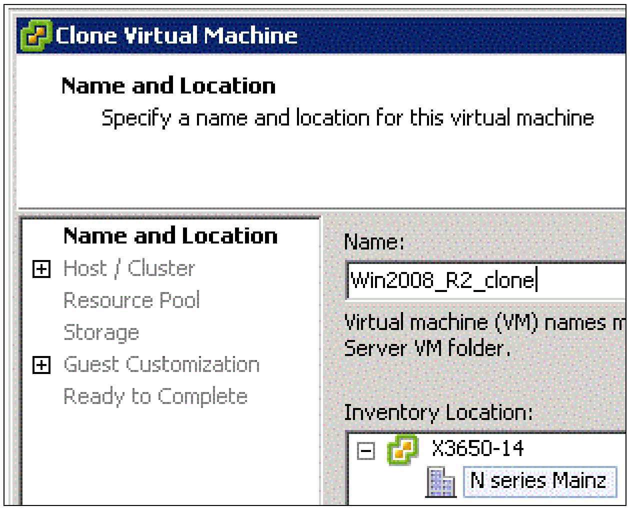


Figure 8-4 Cloning a virtual machine

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**.



Clone Virtual Machine

Name and Location

Specify a name and location for this virtual machine

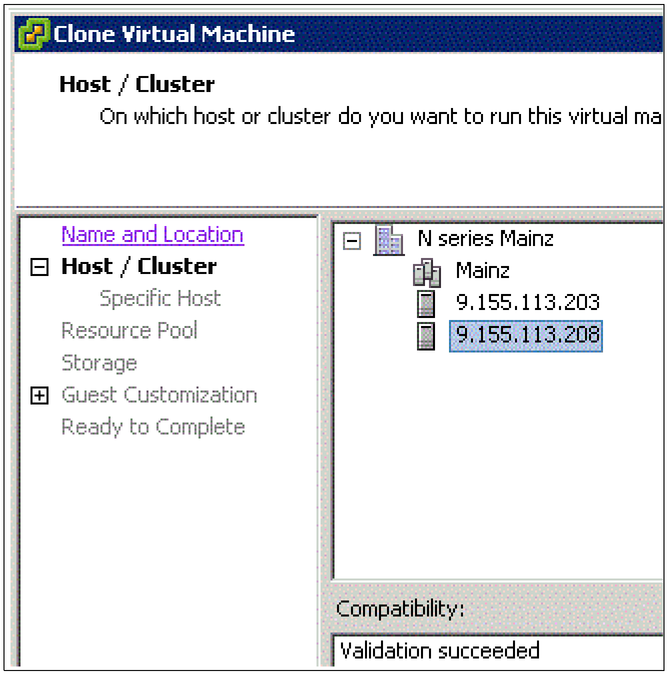
Name: Win2008_R2_clone

Virtual machine (VM) names m
Server VM folder.

Inventory Location:

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**.



Clone Virtual Machine

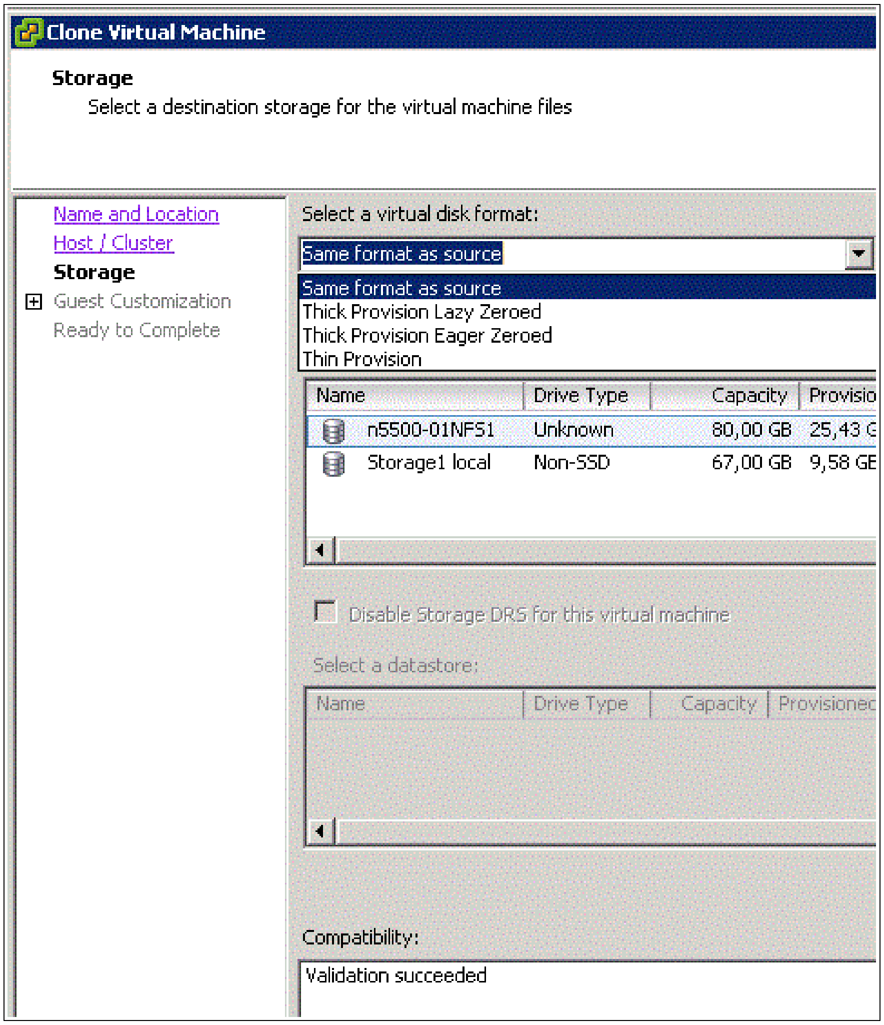
Host / Cluster

On which host or cluster do you want to run this virtual ma

Compatibility: Validation succeeded

Figure 8-6 Selecting a host and check if the validation succeeded

4. In the Choose a Datastore and Disk Format 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**.



Storage

Select a destination storage for the virtual machine files

Select a virtual disk format: Same format as source

Name	Drive Type	Capacity	Provisio
n5500-01NFS1	Unknown	80,00 GB	25,43 G
Storage1 local	Non-SSD	67,00 GB	9,58 GE

☐ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisionec

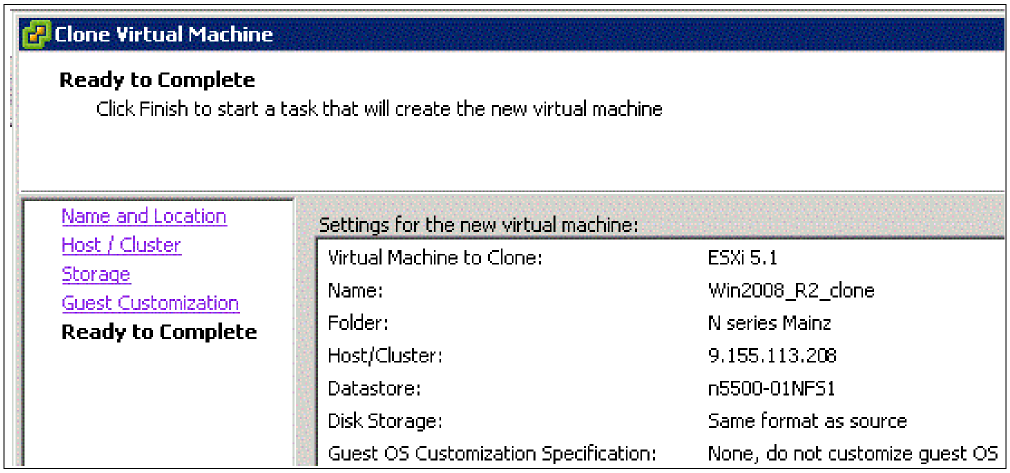
Compatibility:

Validation succeeded

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. In the Ready to Complete New Virtual Machine window, in Figure 8-8, 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**.



Clone Virtual Machine

Ready to Complete

Click Finish to start a task that will create the new virtual machine

Settings for the new virtual machine:

Virtual Machine to Clone:	ESXi 5.1
Name:	Win2008_R2_clone
Folder:	N series Mainz
Host/Cluster:	9.155.113.208
Datastore:	n5500-01NFS1
Disk Storage:	Same format as source
Guest OS Customization Specification:	None, do not customize guest OS

Figure 8-8 Verifying the options to create a new cloned virtual machine

7. After the Clone Virtual Machine is completed on the Recent Tasks pane of the vCenter, you will have your clone as shown in Figure 8-9. It is ready to be started and modified as necessary.

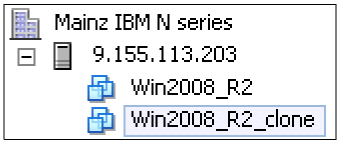
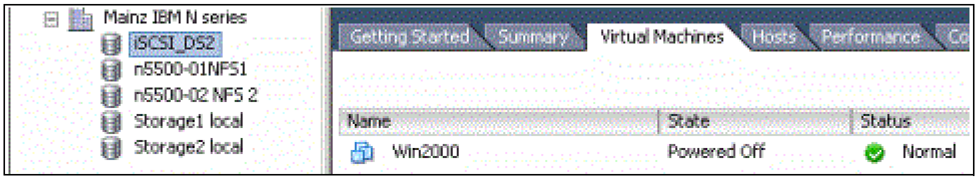


Figure 8-9 Cloned VM ready to be used

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 shown in Figure 8-10.

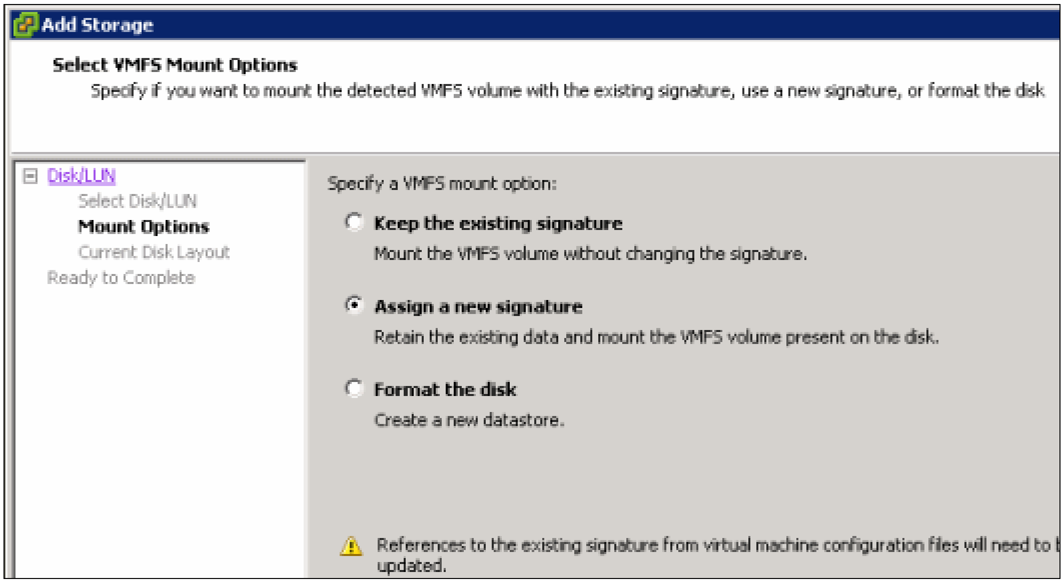


Name	State	Status
Win2000	Powered Off	Normal

Figure 8-10 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.
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 8-11.



Add Storage

Select VMFS Mount Options

Specify if you want to mount the detected VMFS volume with the existing signature, use a new signature, or format the disk

Specify a VMFS mount option:

○ **Keep the existing signature**
Mount the VMFS volume without changing the signature.

● **Assign a new signature**
Retain the existing data and mount the VMFS volume present on the disk.

○ **Format the disk**
Create a new datastore.

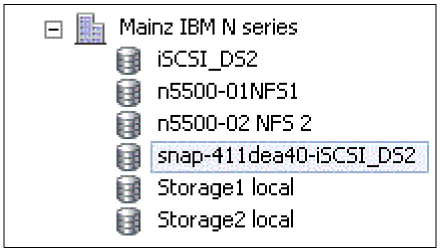
⚠ References to the existing signature from virtual machine configuration files will need to b
updated.

Figure 8-11 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 8-12.



⊟ Mainz IBM N series
- iSCSI_DS2
- n5500-01NFS1
- n5500-02 NFS 2
- snap-411dea40-iSCSI_DS2
- Storage1 local
- Storage2 local

Figure 8-12 New datastore name related to the cloned datastore

2. Right-click the new datastore Figure 8-13, 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.

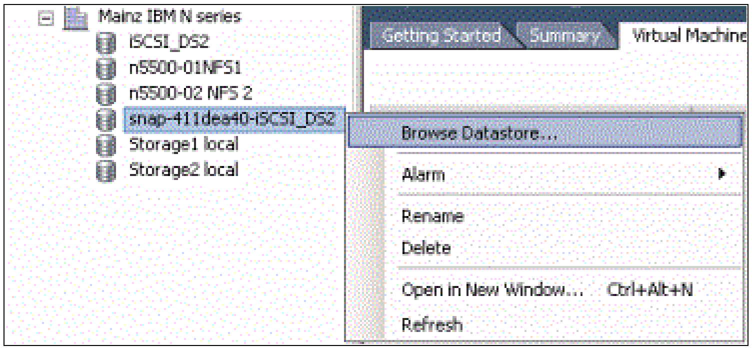
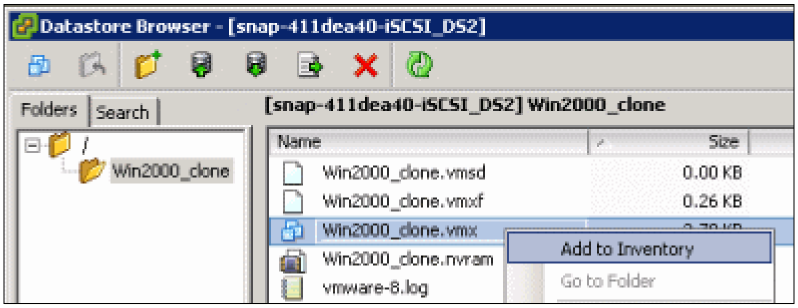


Figure 8-13 Browsing the cloned datastore

3. In the left pane of the Datastore Browser window (Figure 8-14), select one of the guests. In the right pane, right-click the **.vmx** file and select **Add to Inventory**.

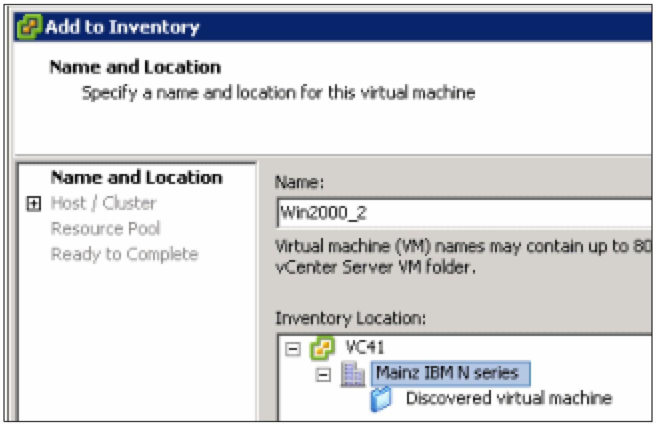

Datastore Browser - [snap-411dea40-iSCSI_DS2]

[snap-411dea40-iSCSI_DS2] Win2000_clone

Name	Size
Win2000_clone.vmsd	0.00 KB
Win2000_clone.vmxf	0.26 KB
Win2000_clone.vmx	
Win2000_clone.nvram	
vmware-8.log	

Figure 8-14 Adding a Virtual Machine to inventory

4. In the Add Inventory Wizard (Figure 8-15), provide a name for the new guest, select the inventory location, and click **Next**.


Add to Inventory

Name and Location

Specify a name and location for this virtual machine

Name:

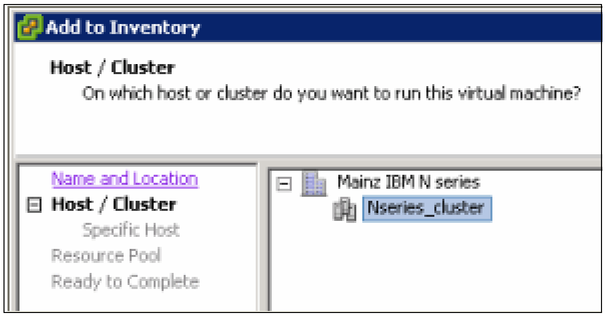
Win2000_2

Virtual machine (VM) names may contain up to 80
vCenter Server VM folder.

Inventory Location:

Figure 8-15 Providing a name to the virtual machine being added

5. In the Select the Host or Cluster panel (Figure 8-16), select a host or cluster. Click **Next**.



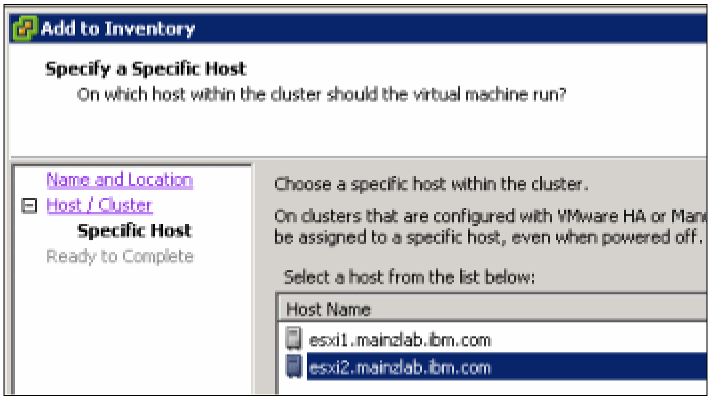
Add to Inventory

Host / Cluster

On which host or cluster do you want to run this virtual machine?

Figure 8-16 Selecting a cluster

6. In the Specify a Specific Host panel (Figure 8-17), select a specific host in a cluster that was selected. Click **Next**.



Add to Inventory

Specify a Specific Host

On which host within the cluster should the virtual machine run?

Choose a specific host within the cluster.

On clusters that are configured with VMware HA or Man
be assigned to a specific host, even when powered off.

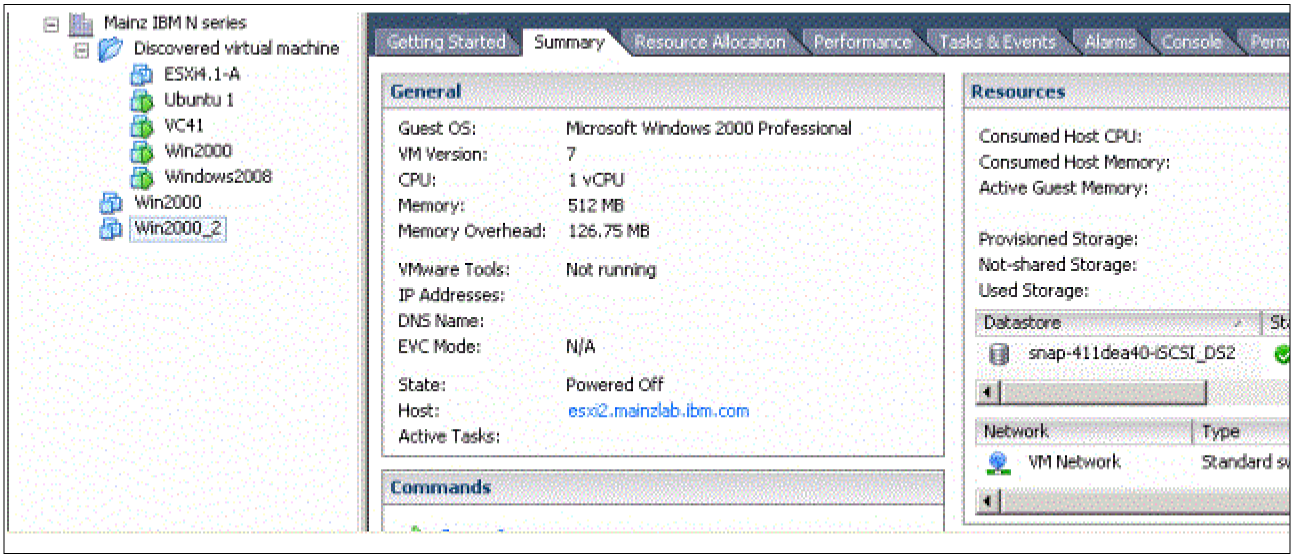
Select a host from the list below:

Host Name
esxi1.mainzlab.ibm.com
esxi2.mainzlab.ibm.com

Figure 8-17 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 8-18.



General

Guest OS: Microsoft Windows 2000 Professional
VM Version: 7
CPU: 1 vCPU
Memory: 512 MB
Memory Overhead: 126.75 MB

VMware Tools: Not running
IP Addresses:
DNS Name:
EVC Mode: N/A

State: Powered Off
Host: esxi2.mainzlab.ibm.com
Active Tasks:

Resources

Consumed Host CPU:
Consumed Host Memory:
Active Guest Memory:

Provisioned Storage:
Not-shared Storage:
Used Storage:

Datastore	St
snap-411dea40-iSCSI_DS2	

Network	Type
VM Network	Standard s

Figure 8-18 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.

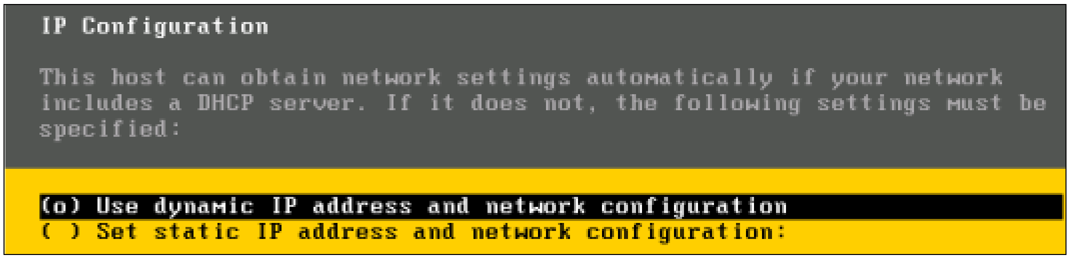
8.5 Cloning VMware ESXi servers

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 ESXi 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 shown in Figure 8-19, and click **OK**.

      Here we are changing the server to be the image to DHCP, so the clones generated from it will not conflict when starting.

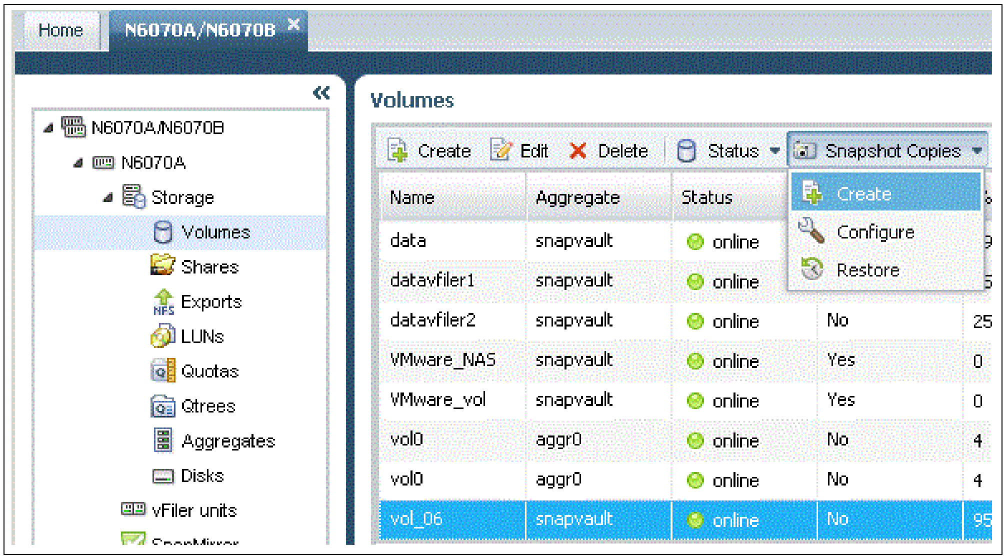


```
IP Configuration

This host can obtain network settings automatically if your network
includes a DHCP server. If it does not, the following settings must be
specified:

(o) Use dynamic IP address and network configuration
( ) Set static IP address and network configuration:
```

Figure 8-19 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 IBM N series System Manager, take a Snapshot of the volume that contains the LUN that you want to clone, as shown in Figure 8-20.



Name	Aggregate	Status		%
data	snapvault	online		9
datavfiler1	snapvault	online		5
datavfiler2	snapvault	online	No	25
VMware_NAS	snapvault	online	Yes	0
VMware_vol	snapvault	online	Yes	0
vol0	aggr0	online	No	4
vol0	aggr0	online	No	4
vol_06	snapvault	online	No	95

Figure 8-20 Taking a Snapshot for the golden image

5. Create a LUN clone by using the IBM N series VSC CLI as Example 8-1.

Example 8-1 Creating a LUN clone

```
N6070A> lun clone create /vol/vol_06/lun_06_clone -b /vol/vol_06/lun_06 snapshot_vol_06
```

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

```
N6070A> lun clone split start /vol/vol_06/lun_06_clone
N6070A> Tue Nov  6 01:39:13 CET [N6070A:lun.clone.split.started:info]: Clone spl
it was started on LUN /vol/vol_06/lun_06_clone.
Tue Nov  6 01:39:14 CET [N6070A:lun.clone.split.completed:info]: Clone split was
completed on LUN /vol/vol_06/lun_06_clone.
```

Put the original host back in service by undoing the modifications that you made.

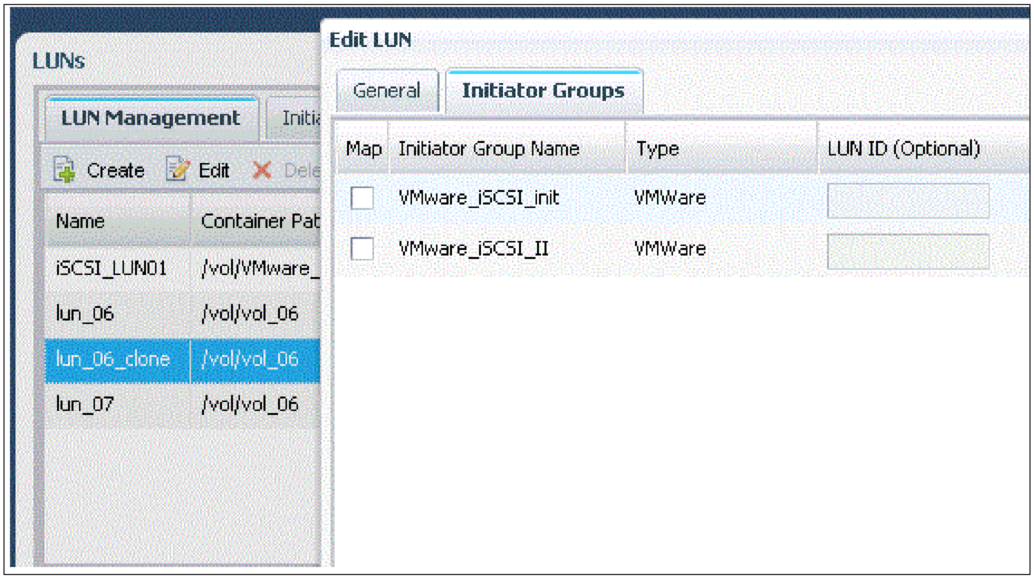
Now that you have a stand-alone golden image, continue as though it were days or months later and you now want to deploy a new VMware ESXi server:

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

```
N6070A> snap create -V vol_06 vol_06_getclone
N6070A> lun clone create /vol/vol_06/lun_07 -b /vol/vol_06/lun_06 vol_06_getclone
Thu May  1 09:15:07 MST [N6070A: lun.clone.created:info]: Created Clone
/vol/vol_06/lun_07 of LUN /vol/vol_06/.snapshot/vol_06_getclone/vol_06
N6070A> lun clone split start /vol/vol_06/lun_07
N6070A> Tue Nov  6 01:56:08 CET [N6070A:lun.clone.split.started:info]: Clone spl
it was started on LUN /vol/vol_06/lun_07.
Tue Nov  6 01:56:08 CET [N6070A:lun.clone.split.completed:info]: Clone split was
completed on LUN /vol/vol_06/lun_07.
```

2. Map the LUN to the new host:
   a. Right-click the desired LUN → **Edit** and at the Edit LUN panel of the IBM N series System Manager (Figure 8-21), clear the **Map** check box for the current Initiator Group and select a different Initiator. In this panel, you can also 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 **Save and Close**.

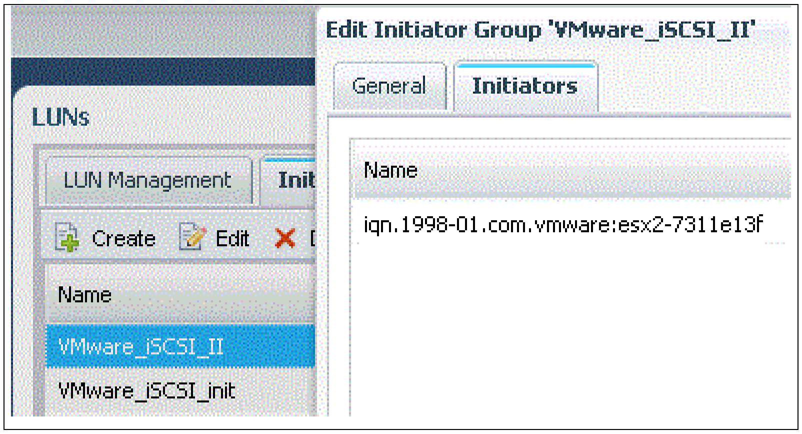


Name	Container Pat
iSCSI_LUN01	/vol/VMware_
lun_06	/vol/vol_06
lun_06_clone	/vol/vol_06
lun_07	/vol/vol_06

Map	Initiator Group Name	Type	LUN ID (Optional)
□	VMware_iSCSI_init	VMWare	
□	VMware_iSCSI_II	VMWare	

Figure 8-21   Edit LUN and select LUN ID panel

   b. In the Edit Initiator Group panel, add the server to map the cloned LUN and click **Save and Close**.

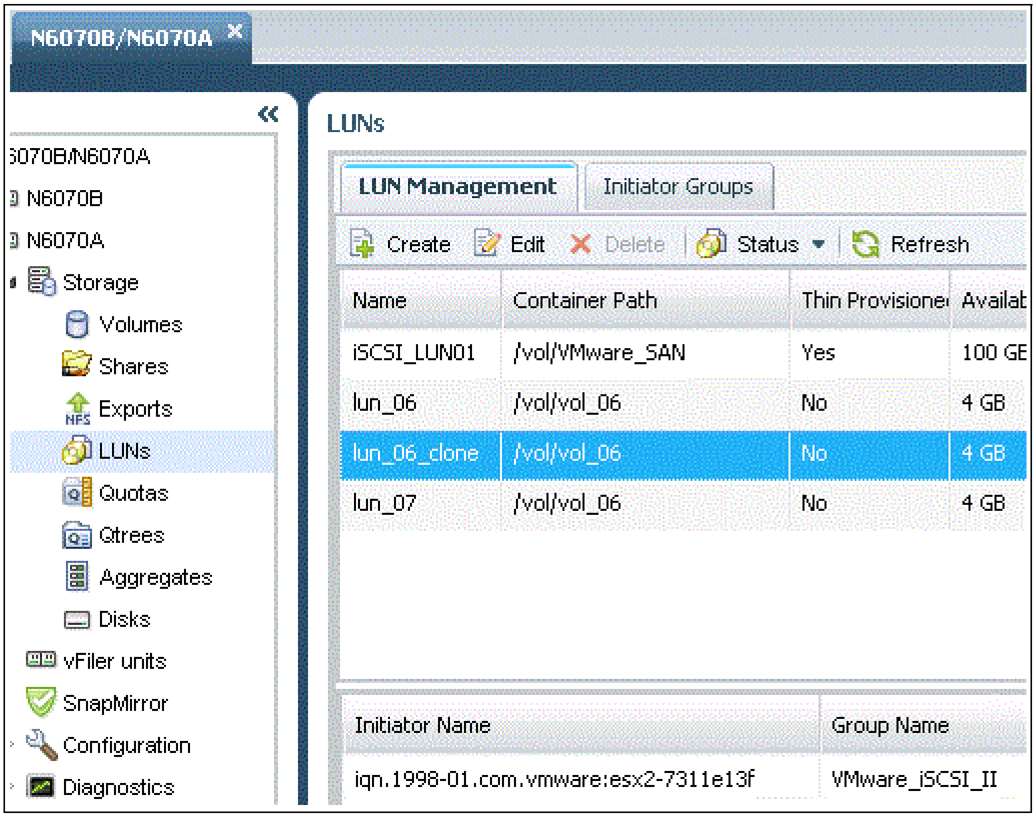


Name
VMware_iSCSI_II
VMware_iSCSI_init

Name
iqn.1998-01.com.vmware:esx2-7311e13f

Figure 8-22   LUN Map Edit Initiator Group panel

3. After applying the LUN ID to the map, under LUNs in the right pane of the IBM N series System Manager, click **LUN Management**. You can now see your new LUN mapped to the new host, as shown in Figure 8-23. Notice that the LUN ID on which the LUN is mapped is 0.



Name	Container Path	Thin Provisione	Availat
iSCSI_LUN01	/vol/VMware_SAN	Yes	100 GE
lun_06	/vol/vol_06	No	4 GB
lun_06_clone	/vol/vol_06	No	4 GB
lun_07	/vol/vol_06	No	4 GB

Initiator Name	Group Name
iqn.1998-01.com.vmware:esx2-7311e13f	VMware_iSCSI_II

Figure 8-23 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 Chapter 5, “Installing the VMware ESXi 5.1 using N series storage” on page 59.

Important: To clone servers, you must ensure that they have the same hardware.

9

Configuring snapshots

VMware backups need to be planned carefully while taking into consideration your environment design. You might be backing up data for various reasons, with each backup requiring a different strategy, such as recovery of lost data or archiving. This chapter provides help with the implementation of snapshots, which can be very useful in data recovery policies. It includes the following topics:

- Storage considerations
- Taking a snapshot
- Scheduling snapshots

© Copyright IBM Corp. 2013. All rights reserved.

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

VMware snapshots are a valuable tool to manage the environment, but they do not cover all the restore and performance possibilities.

To understand this idea, it is necessary 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 instead of the C.vmdk. For each read or write operation, it is necessary check two different files, the original and the -00000x.vmdk, to complete the operation. It might 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 maintaining long term snapshots and keep taking new ones is the access of multiple files to get the information 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.

One last point to consider is that snapshots do not cover complete disaster recovery. If both the primary and secondary sites have serious problems as a natural catastrophe, there would be no data to restore from, as opposed to the common approach of keeping backups stored on media on a remote site.

9.3 Integrating VMware and N series snapshots as a solution

Keeping VMware snapshots of virtual machines is a great point-in-time recovery option, but might cause performance issues. Next we consider how to take advantage of these features while maintaining a system running without impacts.

The solution is to integrate VMware and storage snapshots. In that way, a VMware snapshot is taken, followed by a storage snapshot from the volume containing that VM, and then the VMware snapshot can be deleted, avoiding performance impacts.

> **Important:** This solution does not replace 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).

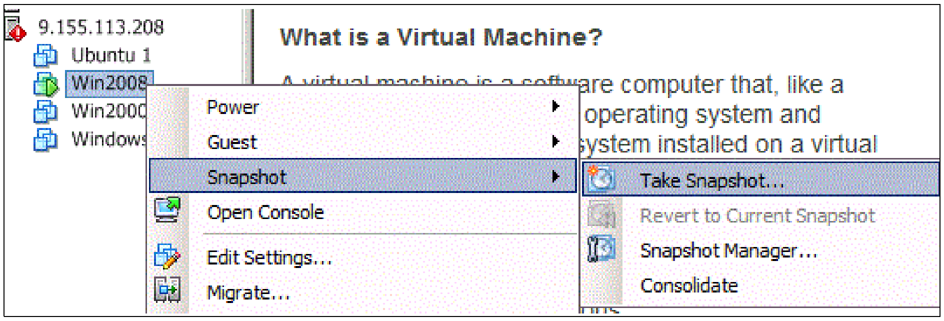
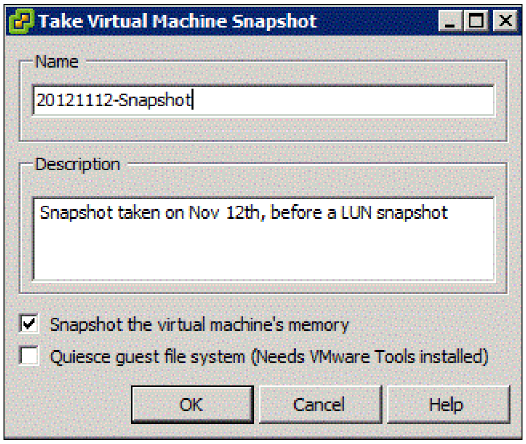


Figure 9-1 Taking a snapshot of a virtual machine

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 memory is written to a file within the datastore, so it is possible to restore the VM with the exact memory content at the moment of the snapshot. Click **OK**.



Name: 20121112-Snapshot

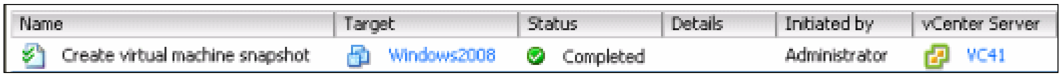
Description: Snapshot taken on Nov 12th, before a LUN snapshot

☑ Snapshot the virtual machine's memory

☐ Quiesce guest file system (Needs VMware Tools installed)

Figure 9-2 VM Snapshot details

4. Verify that the snapshot completed successfully, as shown in Figure 9-3.



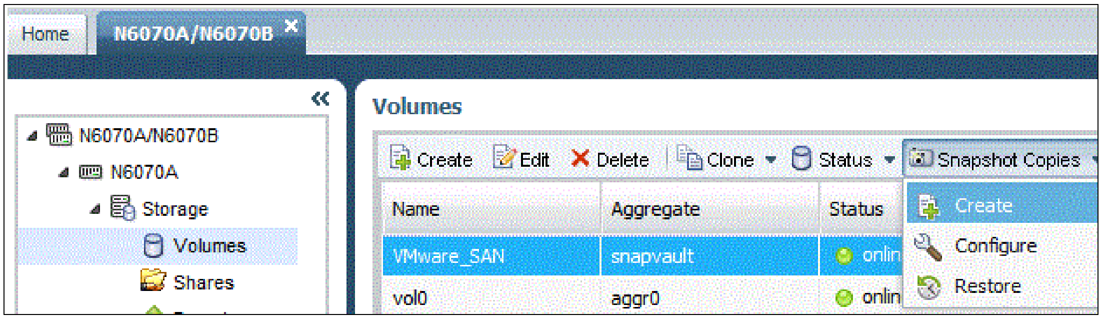
Name	Target	Status	Details	Initiated by	vCenter Server
Create virtual machine snapshot	Windows2008	Completed		Administrator	VC41

Figure 9-3 Guest snapshot complete

Taking a volume snapshot

After the VMware snapshot is completed, take the N series snapshot. To take a snapshot of a volume where the LUN of a datastore reside, use the following steps:

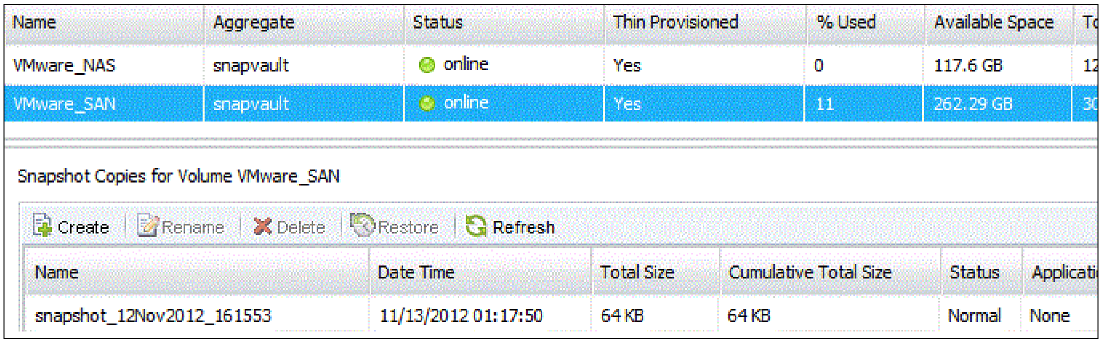
1. Open IBM N series System Manager. Select the **Storage** → **Volumes**, then select the volume, click **Snapshot Copies** → **Create**, as shown in Figure 9-4.



Name	Aggregate	Status
VMware_SAN	snapvault	onlin
vol0	aggr0	onlin

Figure 9-4 Add Snapshot

2. On the next window, provide a name for the snapshot and click **Create**.
3. If the operation is completed successfully, the snapshot will display as shown in Figure 9-5



Name	Aggregate	Status	Thin Provisioned	% Used	Available Space	To
VMware_NAS	snapvault	online	Yes	0	117.6 GB	12
VMware_SAN	snapvault	online	Yes	11	262.29 GB	30

Snapshot Copies for Volume VMware_SAN

Name	Date Time	Total Size	Cumulative Total Size	Status	Applicati
snapshot_12Nov2012_161553	11/13/2012 01:17:50	64 KB	64 KB	Normal	None

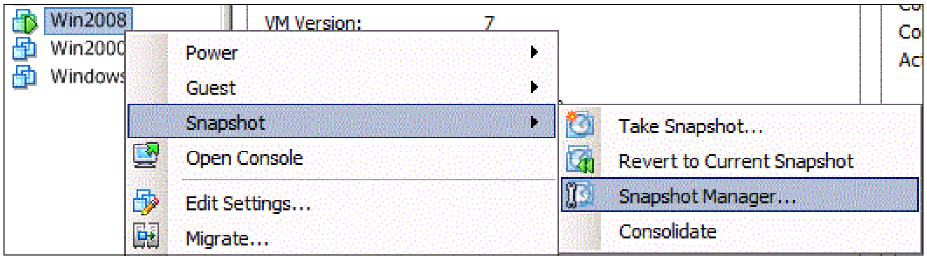
Figure 9-5 Add Snapshot success

Removing the virtual machine snapshot

Follow these steps:

1. Remove the VMware snapshot:

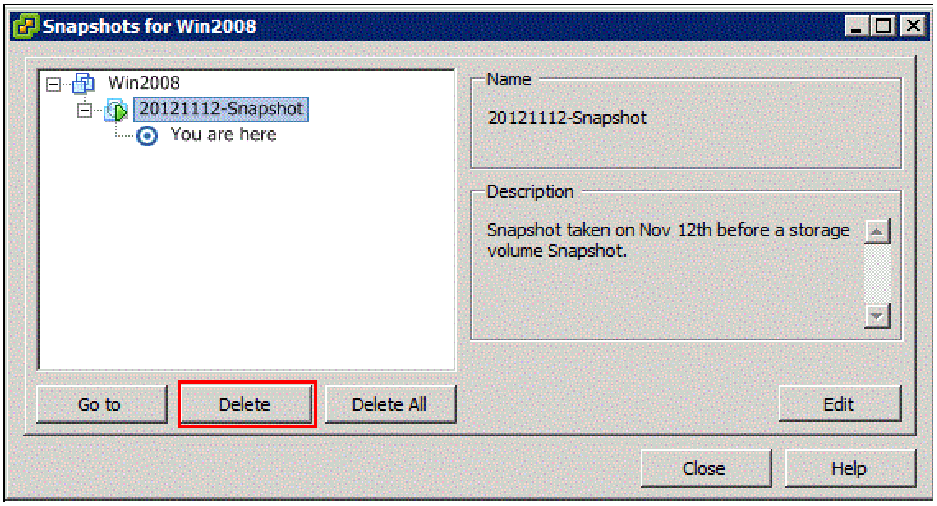
   a. In vCenter, right-click the guest and select **Snapshot** → **Snapshot Manager** as shown in Figure 9-6.



VM Version: 7

Figure 9-6 Guest Snapshot Manager

   b. In the Snapshots window (Figure 9-7), select the snapshot to delete, and click **Delete**.



Name

20121112-Snapshot

Description

Snapshot taken on Nov 12th before a storage volume Snapshot.

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.

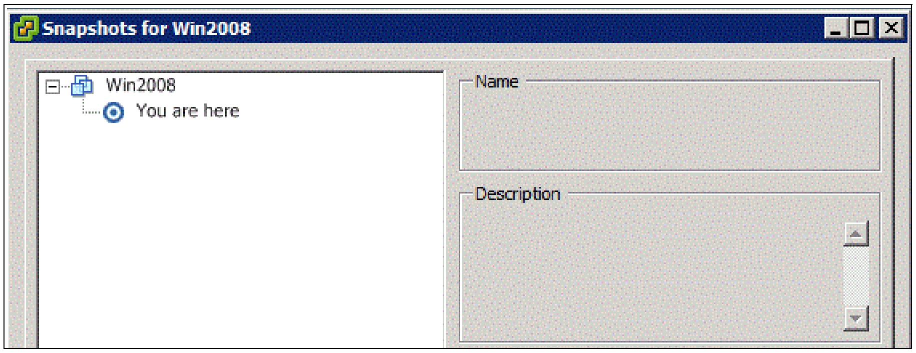


Figure 9-8 Guest Snapshot deleted

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 shown in Figure 9-9.

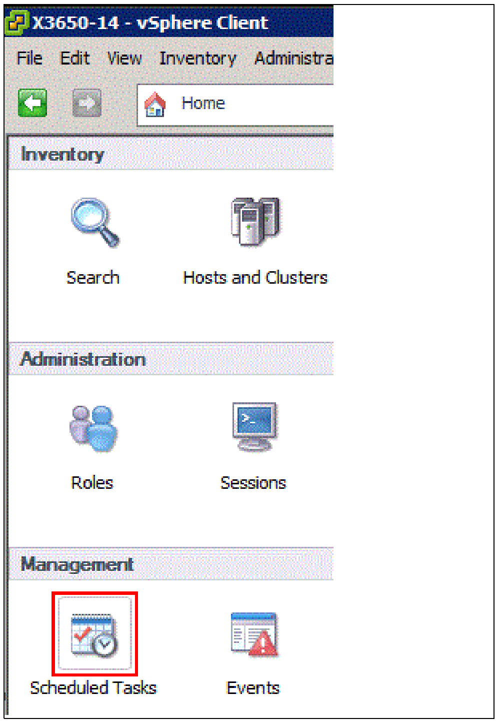
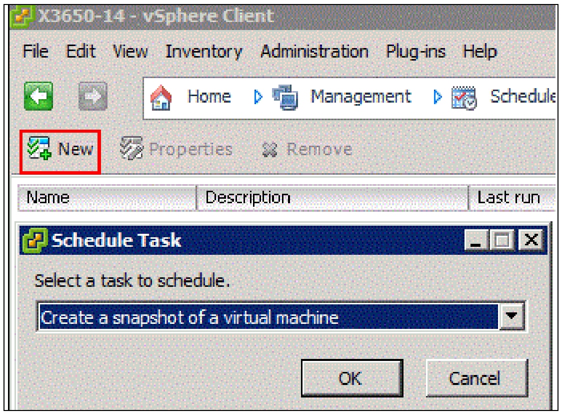


Figure 9-9 Scheduled Tasks

2. Click the **New** button in the left side top of the panel, as shown in Figure 9-10.



Select a task to schedule.

Create a snapshot of a virtual machine

Figure 9-10 Scheduling a new task

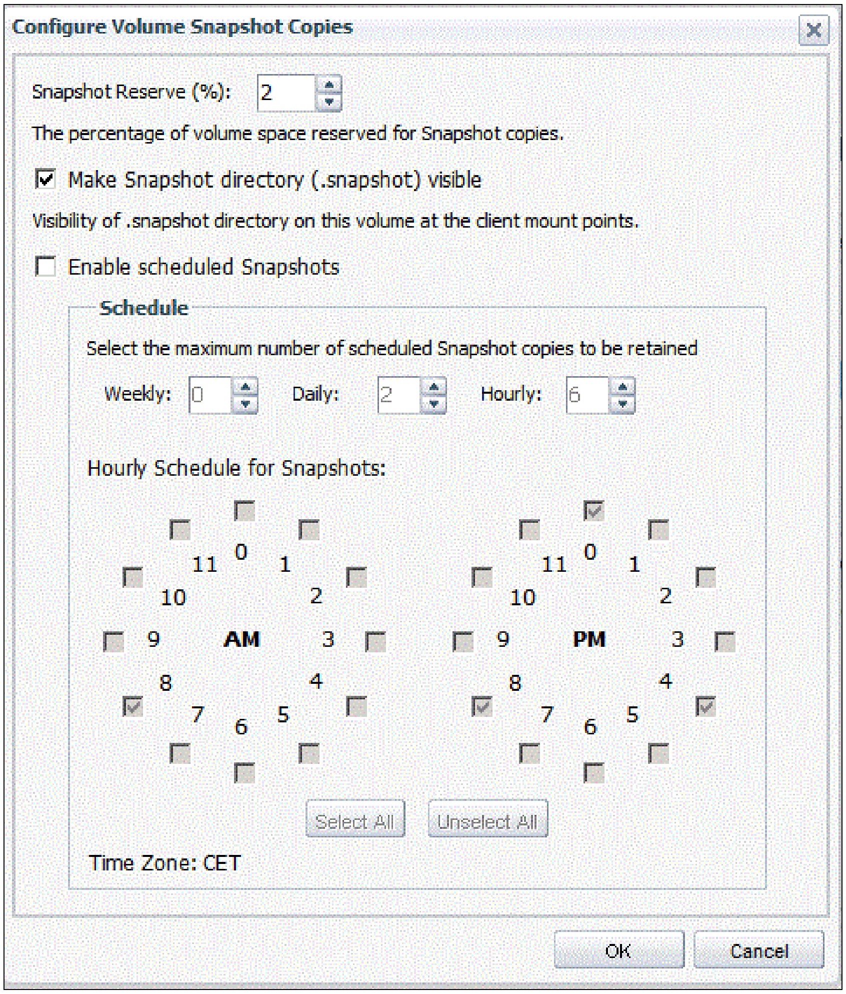
3. Select the virtual machine and click **Next**.
4. Provide a name for the snapshot and select Memory Snapshot also, then click **Next**.
5. Provide a name, date, and time when the task will run, then click **Next**.
6. Enter your email address if you want the vCenter to inform you after the completion 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 command”

```
snap create <vol-name> <snapshot-name>
```

To perform that action using the GUI, open IBM N series System Manager, complete the following steps:

Open IBM N series System Manager, select the **Storage** → **Volumes,** then select the volume, click **Snapshot** → **Configure.** It will display 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**.



Configure Volume Snapshot Copies

Snapshot Reserve (%): 2

The percentage of volume space reserved for Snapshot copies.

☑ Make Snapshot directory (.snapshot) visible

Visibility of .snapshot directory on this volume at the client mount points.

☐ Enable scheduled Snapshots

Schedule

Select the maximum number of scheduled Snapshot copies to be retained

Weekly: 0 Daily: 2 Hourly: 6

Hourly Schedule for Snapshots:

Time Zone: CET

Figure 9-11 Snapshot scheduling options

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

This chapter explains how the 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. It 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

© Copyright IBM Corp. 2013. All rights reserved.

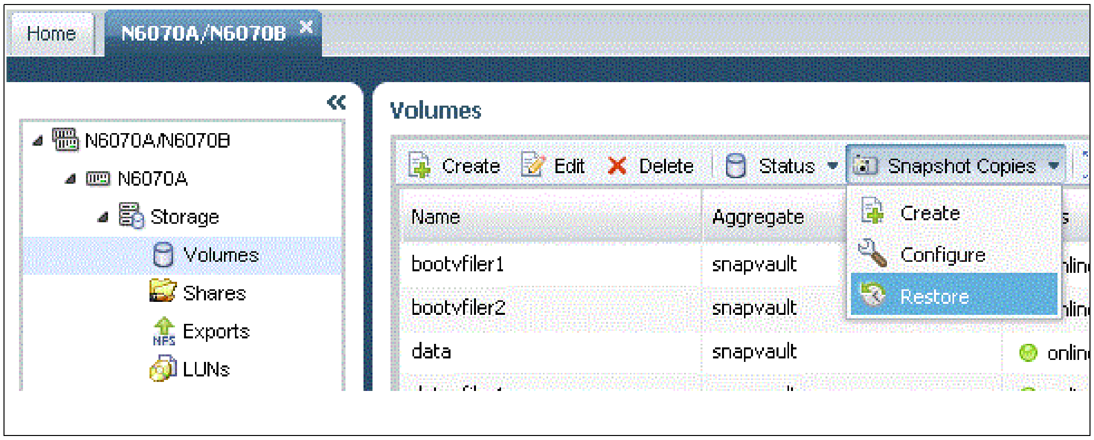
10.1 Restoring a volume

Restoring volumes requires retrieving data from a Snapshot, so you must have at least one in order to restore a volume.

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 IBM N series System Manager as follows:

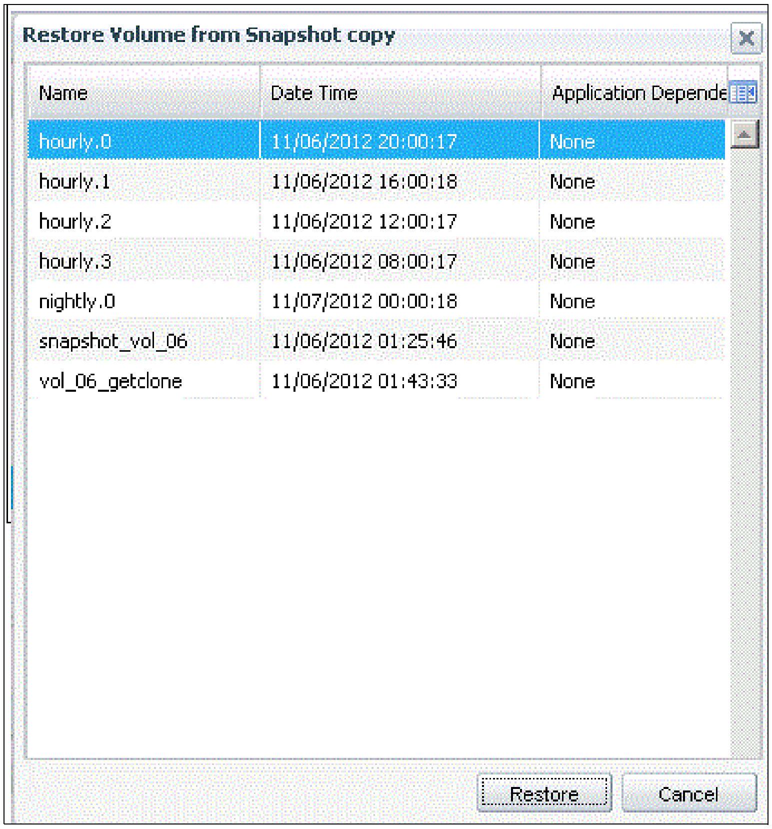
1. Select **Volumes** (highlight the desired volume) → **Snapshot Copies** → **Restore** from the side menu, as shown in Figure 10-1.



Name	Aggregate
bootvfiler1	snapvault
bootvfiler2	snapvault
data	snapvault

Figure 10-1 Volume restore

2. In the Restore Volume from Snapshot copy panel, select the Snapshot copy you want to restore to and click **Restore** as shown in Figure 10-2.

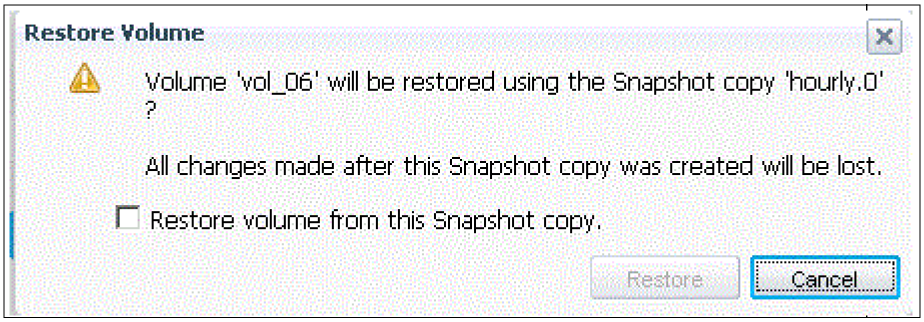


Restore Volume from Snapshot copy

Name	Date Time	Application Depende
hourly.0	11/06/2012 20:00:17	None
hourly.1	11/06/2012 16:00:18	None
hourly.2	11/06/2012 12:00:17	None
hourly.3	11/06/2012 08:00:17	None
nightly.0	11/07/2012 00:00:18	None
snapshot_vol_06	11/06/2012 01:25:46	None
vol_06_getclone	11/06/2012 01:43:33	None

Figure 10-2 Restore Volume List

3. In the Restore Volume confirmation panel select the Restore volume from this Snapshot copy check box and click **Restore** (Figure 10-3).



Restore Volume

Volume 'vol_06' will be restored using the Snapshot copy 'hourly.0' ?

All changes made after this Snapshot copy was created will be lost.

□ Restore volume from this Snapshot copy.

Figure 10-3 Restore Snapshot copy confirmation

10.2 Restoring data from a cloned volume, as with FlexClone

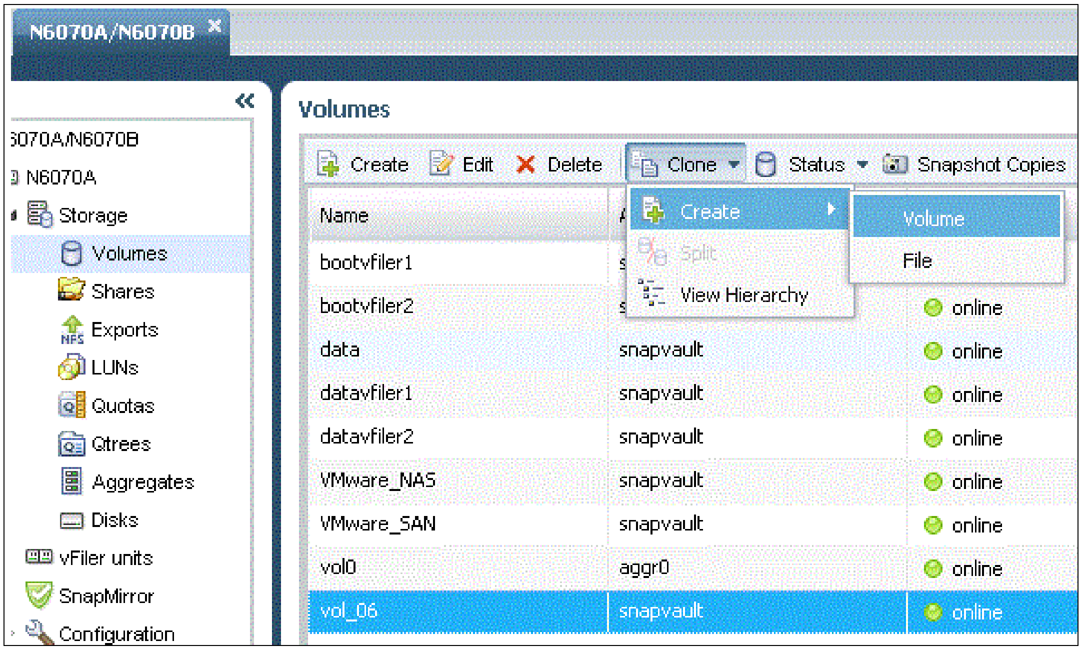
To restore a volume while keeping the existing volume intact, a clone of a Snapshot backup is required. You do this process when only some of the data from a volume was lost or needs to be recovered.

> **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 IBM N series System Manager, complete these steps:

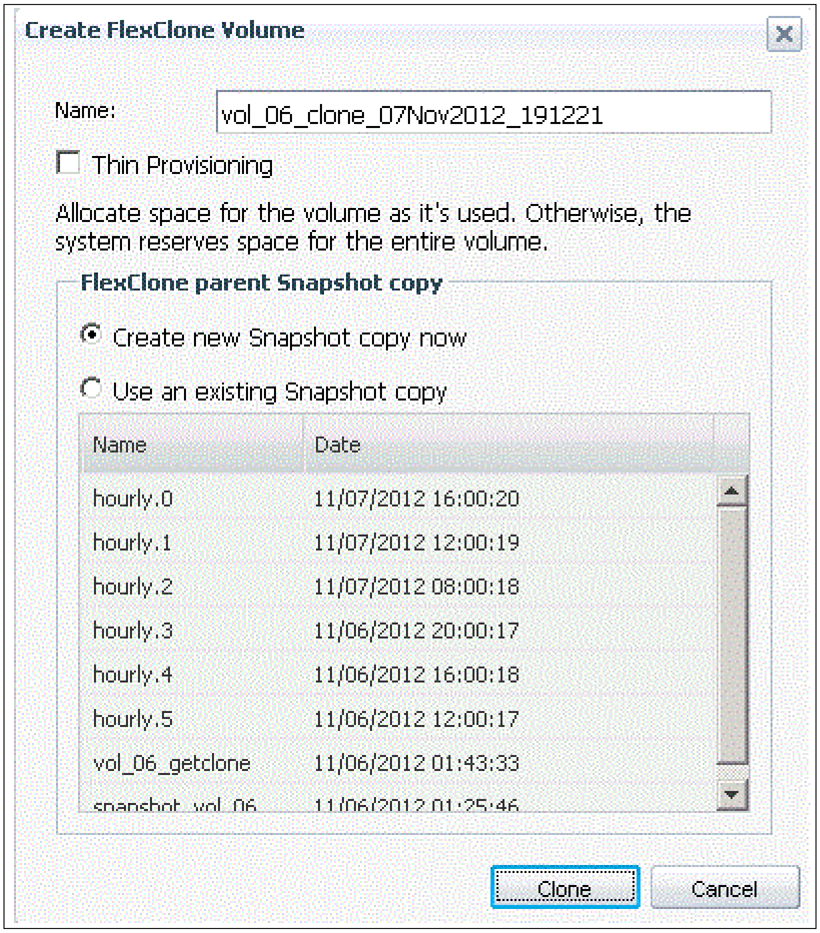
1. In the left navigation pane of the System Manager window (Figure 10-4), select **Volumes,** highlight the desired volume in the right pane and click in **Clone** → **Create** →**Volume**.



Name	A	
bootvfiler1	s	
bootvfiler2	s	online
data	snapvault	online
datavfiler1	snapvault	online
datavfiler2	snapvault	online
VMware_NAS	snapvault	online
VMware_SAN	snapvault	online
vol0	aggr0	online
vol_06	snapvault	online

Figure 10-4 Creating a FlexClone

2. In the Create FlexClone Volume window (Figure 10-5), type the volume clone name and click **Clone**. In this panel, it is also possible specify if you want to create the new cloned volume with Thin Provisioning and if you want to create the new clone from an existing Snapshot or create a new one.



Name: vol_06_clone_07Nov2012_191221

□ Thin Provisioning

Allocate space for the volume as it's used. Otherwise, the system reserves space for the entire volume.

FlexClone parent Snapshot copy

● Create new Snapshot copy now

○ Use an existing Snapshot copy

Name	Date
hourly.0	11/07/2012 16:00:20
hourly.1	11/07/2012 12:00:19
hourly.2	11/07/2012 08:00:18
hourly.3	11/06/2012 20:00:17
hourly.4	11/06/2012 16:00:18
hourly.5	11/06/2012 12:00:17
vol_06_getclone	11/06/2012 01:43:33
snapshot_vol_06	11/06/2012 01:25:46

Figure 10-5 Creating a FlexClone

3. In the Clone a Flexible Volume pane, enter the name of the new clone. Select the volume to be cloned and the Space Guarantee option that you require. Click **Next**.

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 System Manager GUI. 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>
```

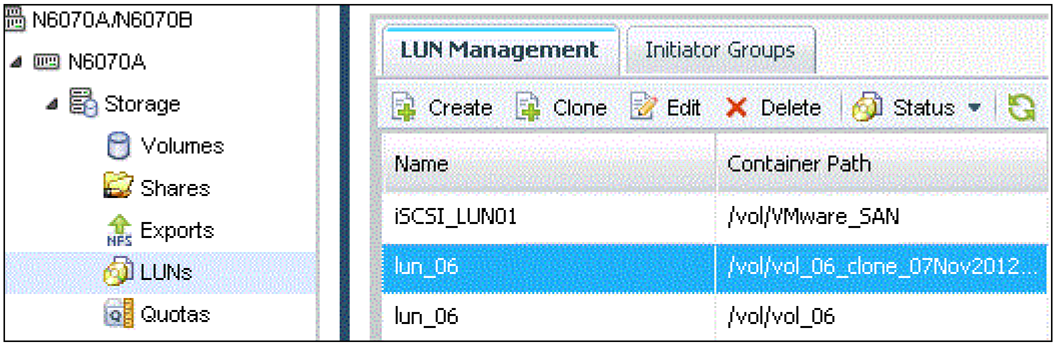
10.2.2 Configuring the cloned LUN to be accessed

After the clone is created, you must bring the LUN to online status and map the LUN to a host or hosts, then create a datastore over it.

Mapping a LUN to hosts

Follow these steps:

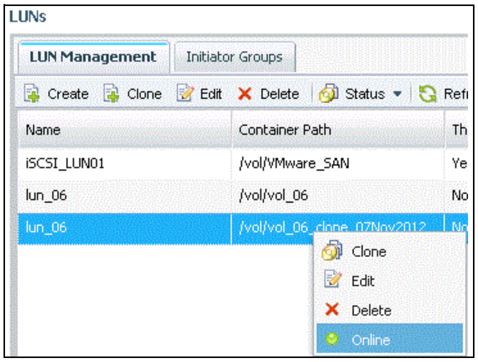
1. In the IBM N series System Manager, in the left navigation pane, select **LUNs,** and you see the cloned LUN in the right pane as shown in Figure 10-6.



Name	Container Path
iSCSI_LUN01	/vol/VMware_SAN
lun_06	/vol/vol_06_clone_07Nov2012...
lun_06	/vol/vol_06

Figure 10-6 The cloned LUN

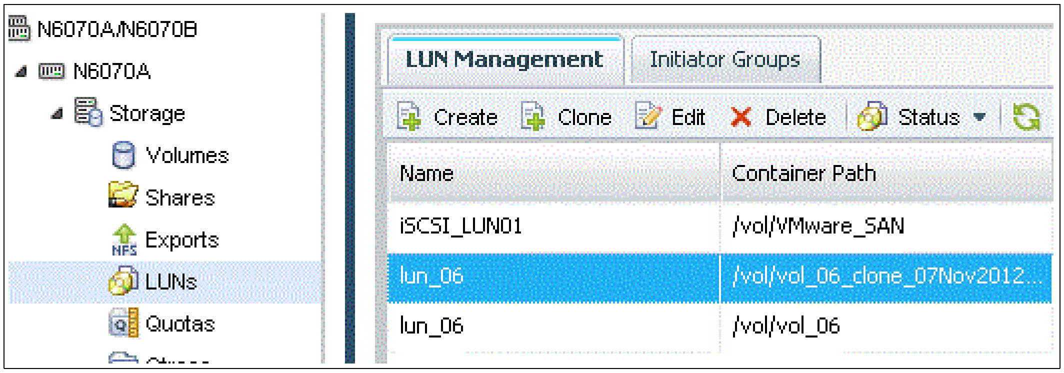
2. Right-click the cloned LUN and click **Online** as shown in Figure 10-7.



Name	Container Path	Th
iSCSI_LUN01	/vol/VMware_SAN	Ye
lun_06	/vol/vol_06	No
lun_06	/vol/vol_06_clone_07Nov2012	Nc

Figure 10-7 Bring LUN online

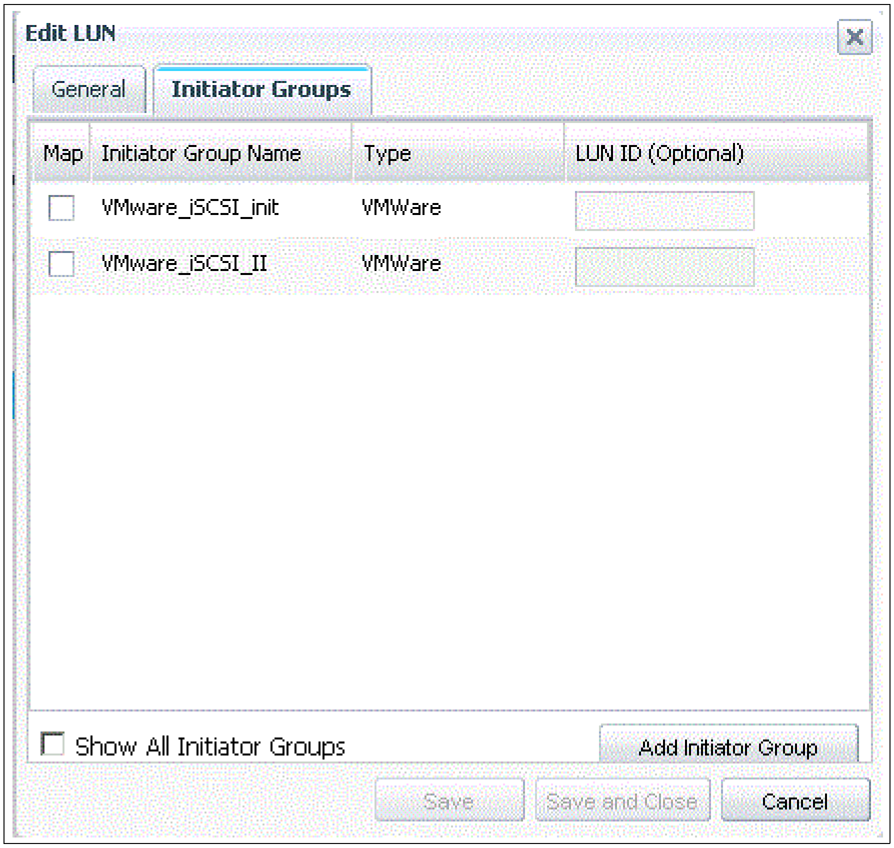
3. Highlight the desired LUN and then → **Edit**, as shown in Figure 10-8. It is not mapped to any host, so we want to configure it.



Name	Container Path
iSCSI_LUN01	/vol/VMware_SAN
lun_06	/vol/vol_06_clone_07Nov2012...
lun_06	/vol/vol_06

Figure 10-8 Edit LUN

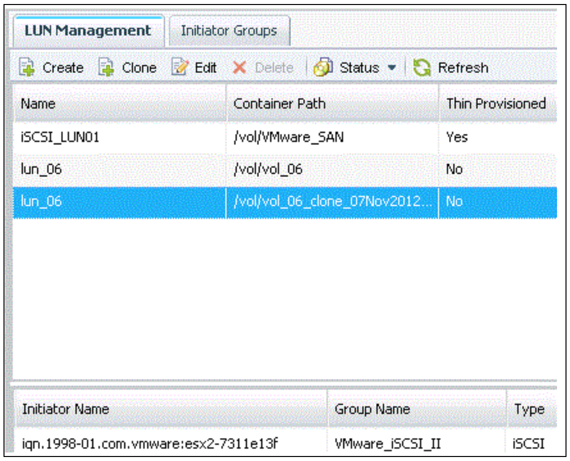
4. Then select the proper Initiator Group you want to map the LUN, type the LUN ID (Optional) and click **Save and Close** (Figure 10-9).



Map	Initiator Group Name	Type	LUN ID (Optional)
☐	VMware_iSCSI_init	VMWare	
☐	VMware_iSCSI_II	VMWare	

Figure 10-9 Add Groups to Map

5. Now you have mapped the LUN and the host or hosts should be able to access it as shown in Figure 10-10.



Name	Container Path	Thin Provisioned
iSCSI_LUN01	/vol/VMware_SAN	Yes
lun_06	/vol/vol_06	No
lun_06	/vol/vol_06_clone_07Nov2012...	No

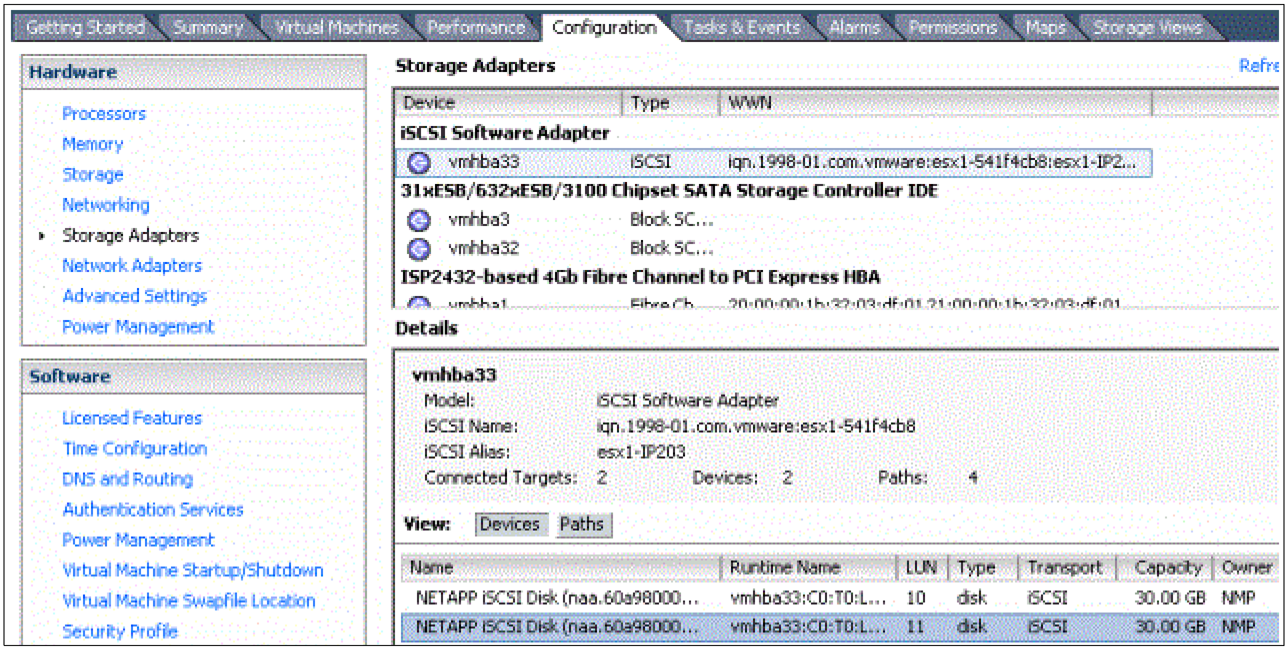
Initiator Name	Group Name	Type
iqn.1998-01.com.vmware:esx2-7311e13f	VMware_iSCSI_II	iSCSI

Figure 10-10 Cloned LUN mapped

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 available on the host, as shown in Figure 10-11. You can identify the new LUN by the LUN ID.



Storage Adapters

Device	Type	WWN
iSCSI Software Adapter		
vmhba33	iSCSI	iqn.1998-01.com.vmware:esx1-541f4cb8:esx1-IP2...
31xESB/632xESB/3100 Chipset SATA Storage Controller IDE		
vmhba3	Block SC...	
vmhba32	Block SC...	
ISP2432-based 4Gb Fibre Channel to PCI Express HBA		
vmhba1	Fibre Ch...	20:00:00:1b:32:03:df:01 21:00:00:1b:32:03:df:01

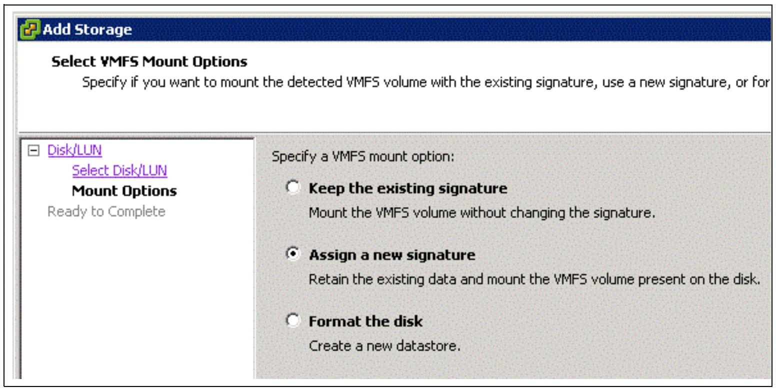
Details

vmhba33
Model: iSCSI Software Adapter
iSCSI Name: iqn.1998-01.com.vmware:esx1-541f4cb8
iSCSI Alias: esx1-IP203
Connected Targets: 2 Devices: 2 Paths: 4

Name	Runtime Name	LUN	Type	Transport	Capacity	Owner
NETAPP iSCSI Disk (naa.60a98000...	vmhba33:C0:T0:L...	10	disk	iSCSI	30.00 GB	NMP
NETAPP iSCSI Disk (naa.60a98000...	vmhba33:C0:T0:L...	11	disk	iSCSI	30.00 GB	NMP

Figure 10-11 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 10-12. That option enables the copy from the cloned datastore into the existing one.



Select VMFS Mount Options

Specify if you want to mount the detected VMFS volume with the existing signature, use a new signature, or for

Specify a VMFS mount option:

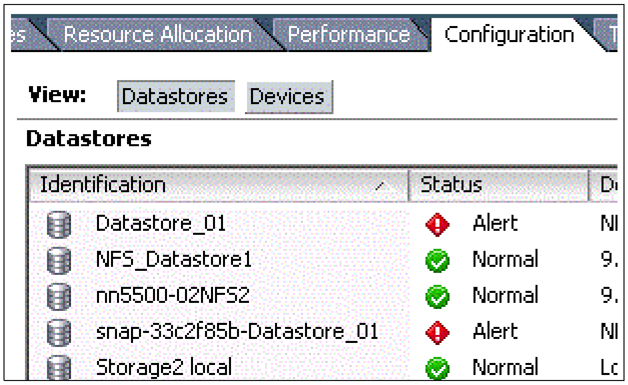
○ **Keep the existing signature**
Mount the VMFS volume without changing the signature.

● **Assign a new signature**
Retain the existing data and mount the VMFS volume present on the disk.

○ **Format the disk**
Create a new datastore.

Figure 10-12 Changing to Assign a new signature

6. In the Ready to Complete panel, observe that a new signature is going to be applied to the LUN. Click **Finish**.
7. After adding the datastore, it will have a name referencing the cloned LUN/datastore, as shown in Figure 10-13.



Datastores

Identification	Status	D
Datastore_01	Alert	N
NFS_Datastore1	Normal	9.
nn5500-02NFS2	Normal	9.
snap-33c2f85b-Datastore_01	Alert	N
Storage2 local	Normal	Lc

Figure 10-13 The cloned LUN creates a datastore referring the original one

10.3 Recovering an entire virtual machine

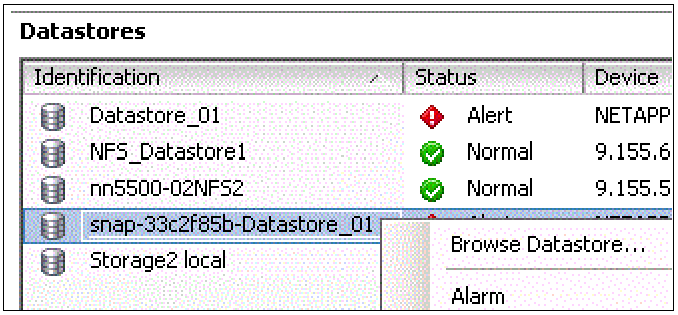
To recover a guest because of data corruption, the original guest files are replaced with the files of the cloned guest created in the previous sections.

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:

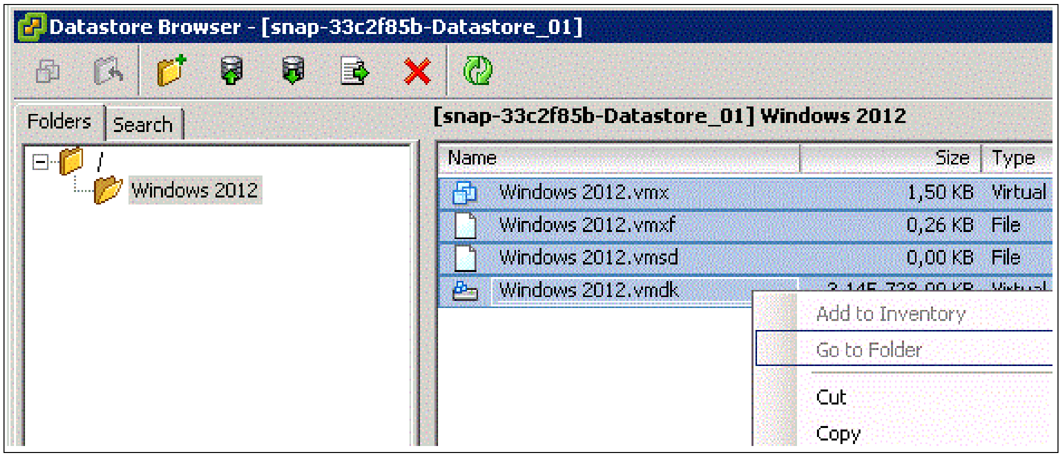
1. Browse the guest datastore, as shown in Figure 10-14.


Datastores

Identification	Status	Device
Datastore_01	Alert	NETAPP
NFS_Datastore1	Normal	9.155.6
nn5500-02NFS2	Normal	9.155.5
snap-33c2f85b-Datastore_01		
Storage2 local		

Figure 10-14 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 shown in Figure 10-15.



Datastore Browser - [snap-33c2f85b-Datastore_01]
Folders
Search
/
Windows 2012
[snap-33c2f85b-Datastore_01] Windows 2012
Add to Inventory
Go to Folder
Cut
Copy

Name	Size	Type
Windows 2012.vmx	1,50 KB	Virtual
Windows 2012.vmxf	0,26 KB	File
Windows 2012.vmsd	0,00 KB	File
Windows 2012.vmdk	3 145 728,00 KB	Virtual

Figure 10-15 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 shown in Figure 10-16.

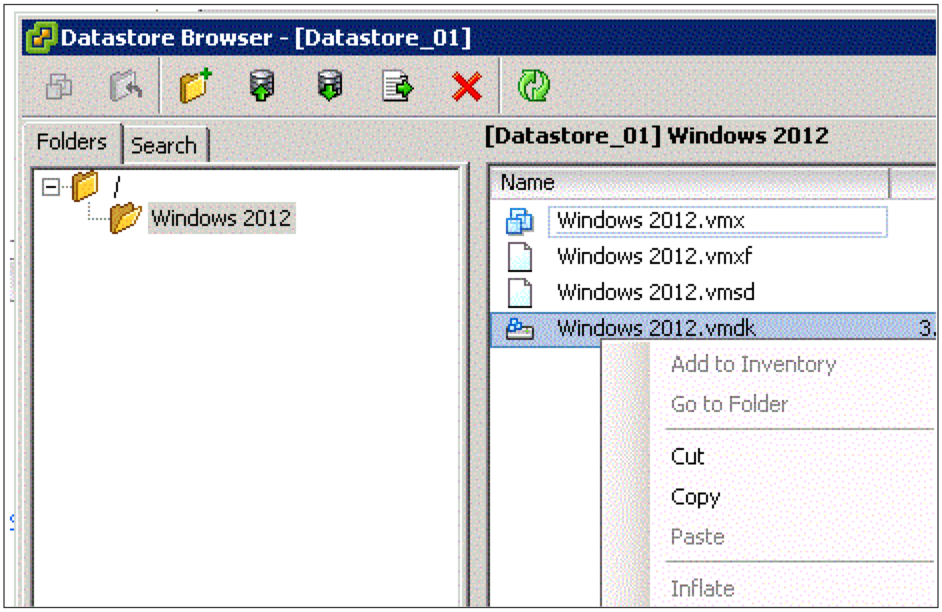
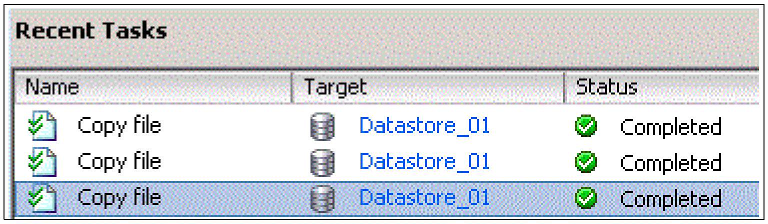


Figure 10-16 Pasting the VM files over the original datastore / VM folder

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 shown in Figure 10-17.



Recent Tasks

Name	Target	Status
Copy file	Datastore_01	Completed
Copy file	Datastore_01	Completed
Copy file	Datastore_01	Completed

Figure 10-17 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.

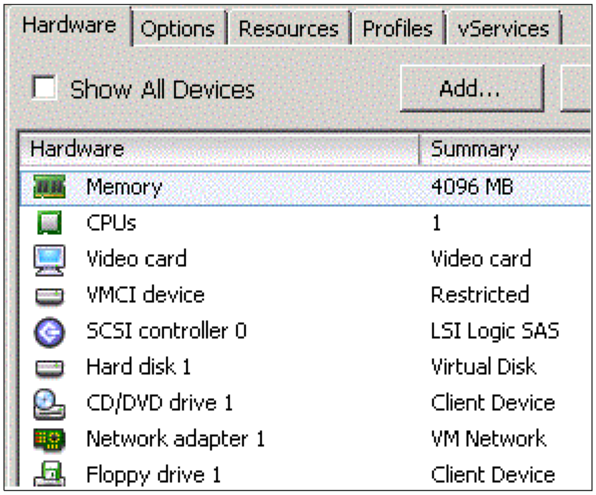
10.4.1 Creating a temporary recovery guest

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 shown in Figure 10-18.

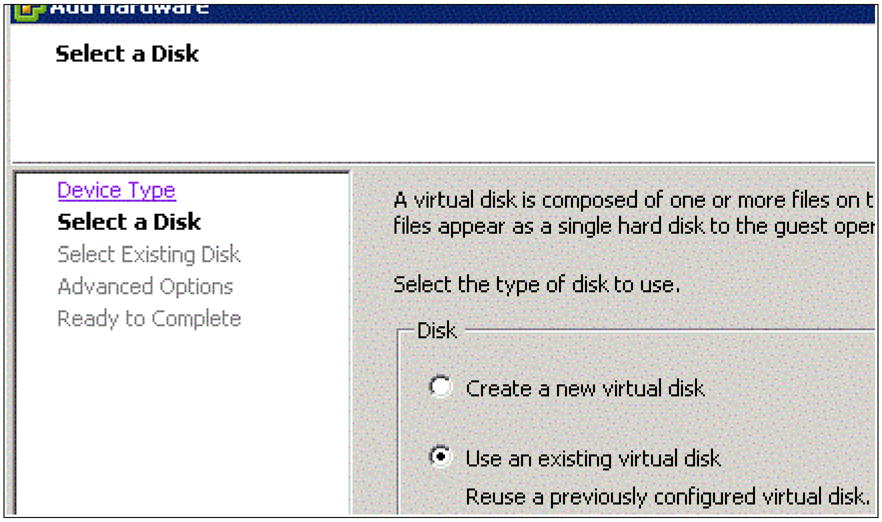


□ Show All Devices

Hardware	Summary
Memory	4096 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
CD/DVD drive 1	Client Device
Network adapter 1	VM Network
Floppy drive 1	Client Device

Figure 10-18 Adding disk to the temporary VM

3. Select **Hard Disk** and click **Next**.
4. Select **Use an existing virtual disk** as shown in Figure 10-19, and click **Next**.



Select a Disk

A virtual disk is composed of one or more files on t
files appear as a single hard disk to the guest oper

Select the type of disk to use.

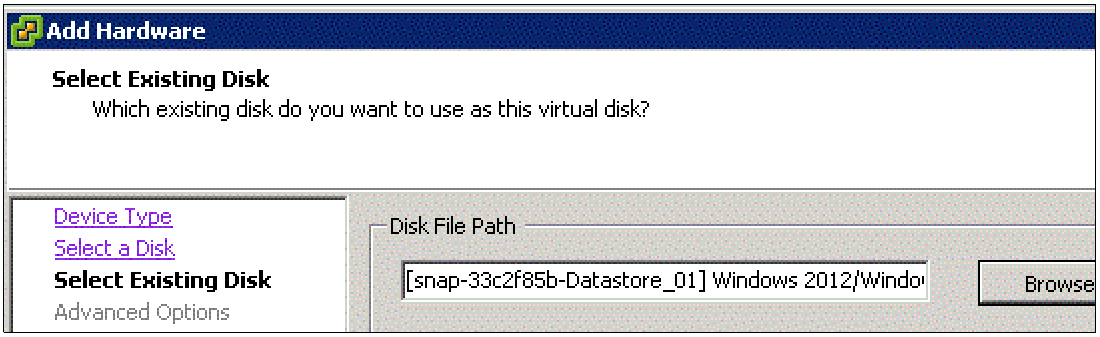
Disk

○ Create a new virtual disk

● Use an existing virtual disk
Reuse a previously configured virtual disk.

Figure 10-19 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 10-20, then click **Next**.

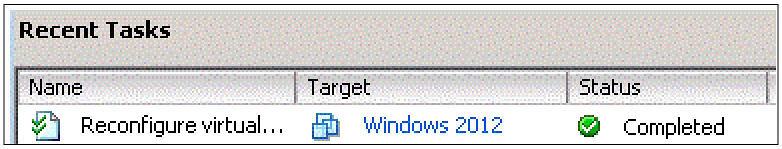


Select Existing Disk
Which existing disk do you want to use as this virtual disk?

Disk File Path
[snap-33c2f85b-Datastore_01] Windows 2012/Windo

Figure 10-20 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 10-21).



Recent Tasks

Name	Target	Status
Reconfigure virtual...	Windows 2012	Completed

Figure 10-21 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 F: in this case. This disk is the cloned disk from where the data is to be recovered (Figure 10-22).

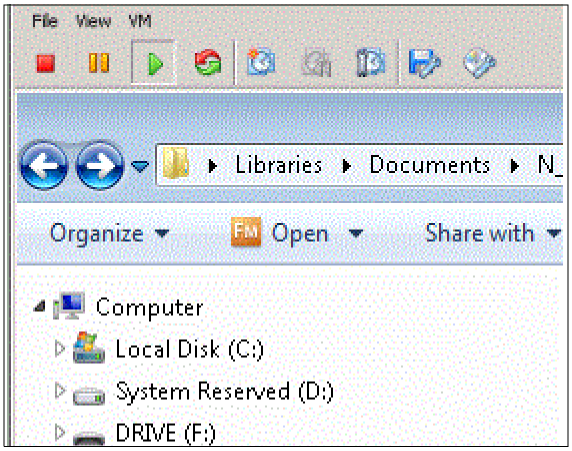
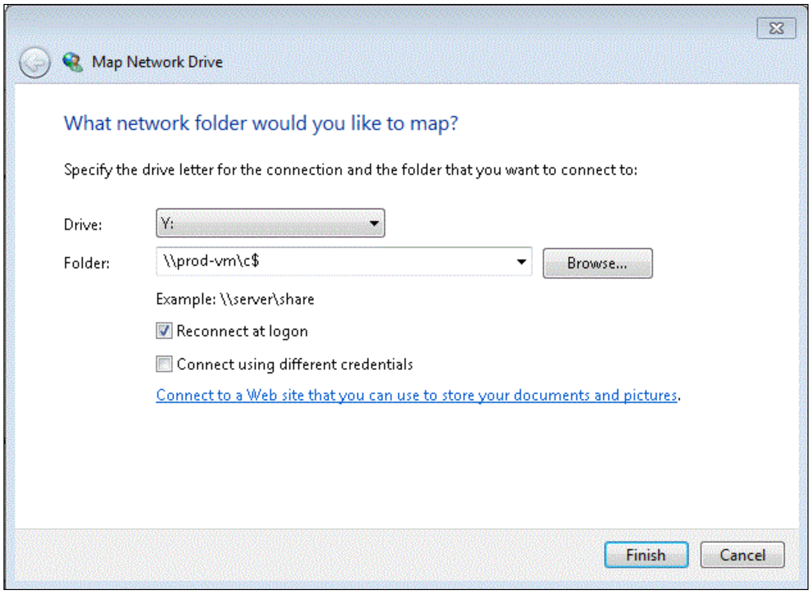


Figure 10-22 The disk from which the data is to be recovered

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 10-23).



What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Y:

Folder: \\prod-vm\c$

Example: \\server\share

☑ Reconnect at logon

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

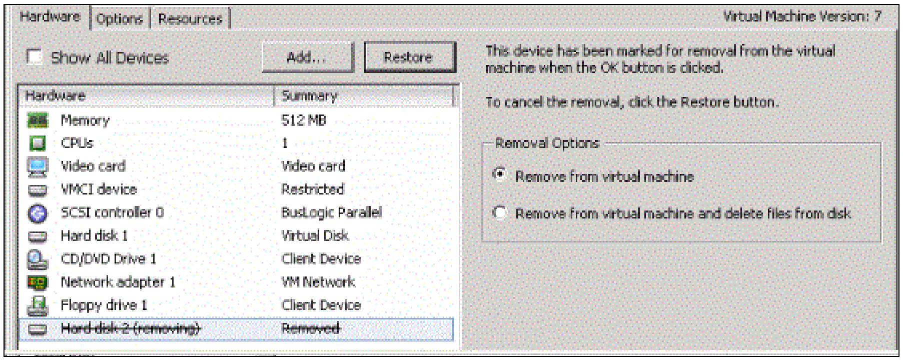
Figure 10-23 Mapping the destination drive on the original virtual machine

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 shown in Figure 10-24, then click **OK**.



Virtual Machine Version: 7

□ Show All Devices

Hardware	Summary
Memory	512 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	BusLogic Parallel
Hard disk 1	Virtual Disk
CD/DVD Drive 1	Client Device
Network adapter 1	VM Network
Floppy drive 1	Client Device
~~Hard disk 2 (removing)~~	~~Removed~~

This device has been marked for removal from the virtual machine when the OK button is clicked.

To cancel the removal, click the Restore button.

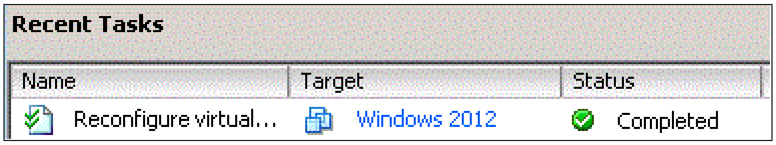
Removal Options

● Remove from virtual machine

○ Remove from virtual machine and delete files from disk

Figure 10-24 Removing the disk from the VM

5. Verify that the Recent Tasks list to confirm that the disk was removed, as shown in Figure 10-25.



Recent Tasks

Name	Target	Status
Reconfigure virtual...	Windows 2012	Completed

Figure 10-25 Completion of disk removal

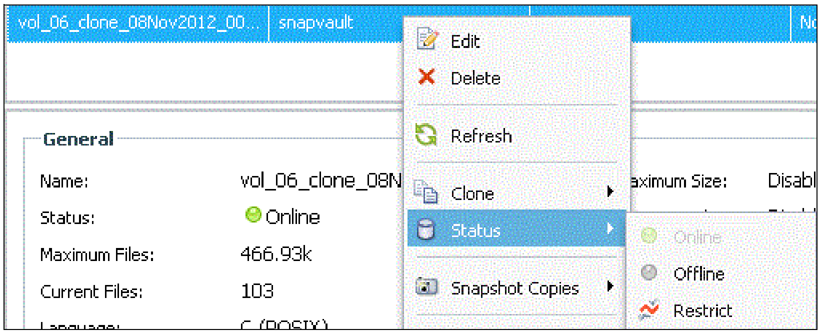
10.4.5 Removing the cloned LUN

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 IBM N series System Manager, from the left navigation pane (Figure 10-26), select **Volumes** → Right-click the cloned volume → **Status** → **Offline** as shown in Figure 10-26.



General

Name: vol_06_clone_08N

Status: Online

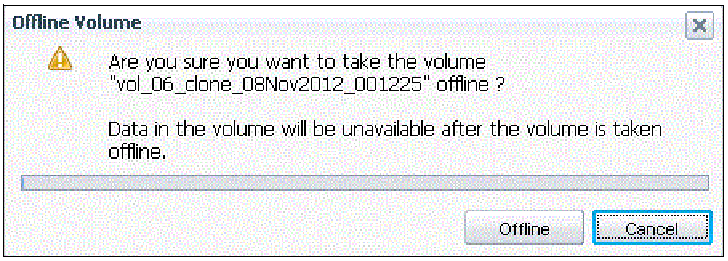
Maximum Files: 466.93k

Current Files: 103

Language: C (POSIX)

Figure 10-26 Selecting the volume and taking it offline

2. Click **Offline** to confirm taking the volume offline and then check the success message on Manage Volumes, as shown in Figure 10-27.



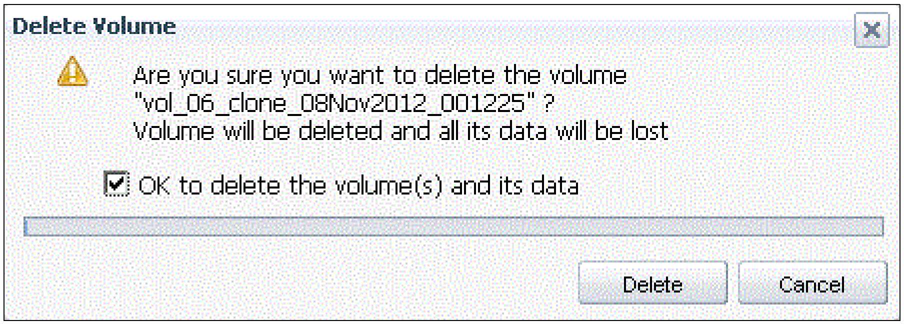
Offline Volume

Are you sure you want to take the volume "vol_06_clone_08Nov2012_001225" offline ?

Data in the volume will be unavailable after the volume is taken offline.

Figure 10-27 Take volume offline

3. Right-click the volume again, but this time, click **Delete**.
4. Mark the check box and click **Delete** to confirm that you want to destroy the volume that is shown in Figure 10-28.



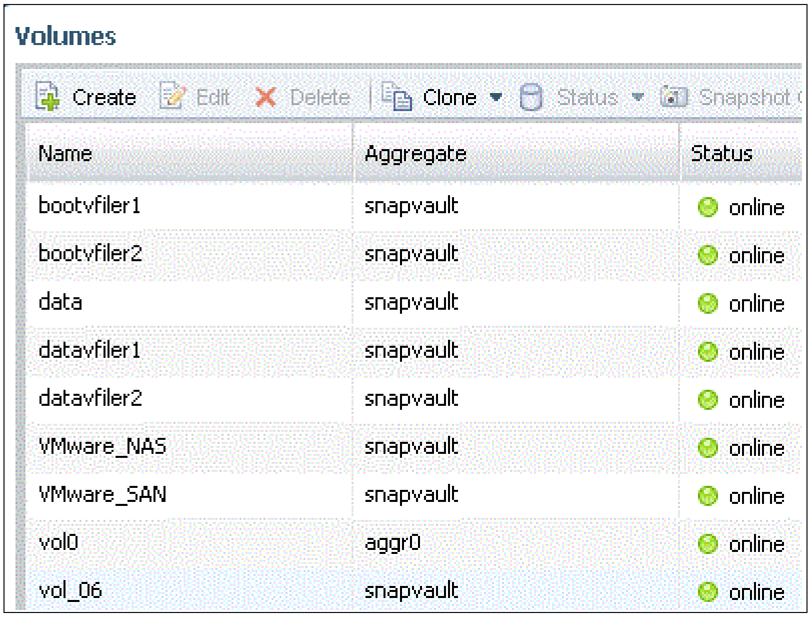
Delete Volume

⚠ Are you sure you want to delete the volume "vol_06_clone_08Nov2012_001225" ?
Volume will be deleted and all its data will be lost

☑ OK to delete the volume(s) and its data

Figure 10-28 Confirm volume deletion

5. Now the Manage Volumes pane (Figure 10-29) indicates that Destroy function was successful, and the volume is not present on the list anymore.

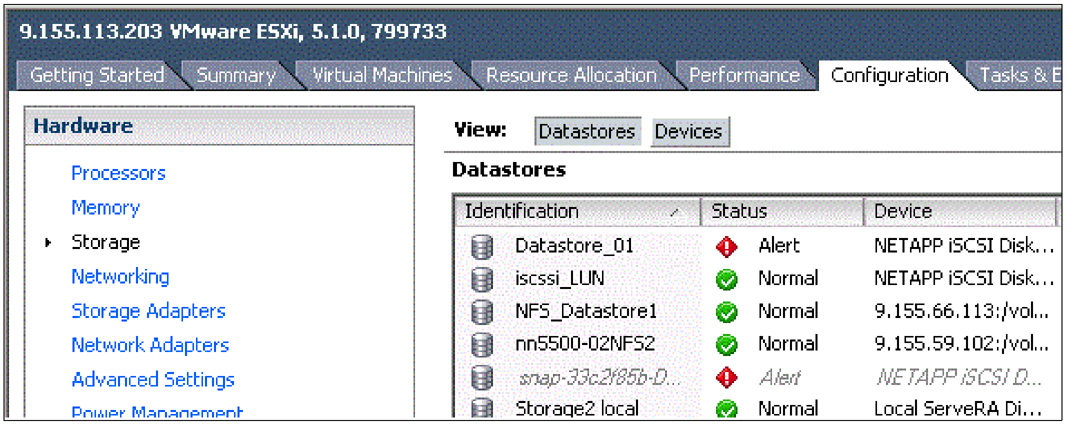


Volumes

Name	Aggregate	Status
bootvfiler1	snapvault	● online
bootvfiler2	snapvault	● online
data	snapvault	● online
datavfiler1	snapvault	● online
datavfiler2	snapvault	● online
VMware_NAS	snapvault	● online
VMware_SAN	snapvault	● online
vol0	aggr0	● online
vol_06	snapvault	● online

Figure 10-29 The success message after destroying the volume

6. You will see the datastore related to that LUN grayed, as it is unavailable (Figure 10-30).



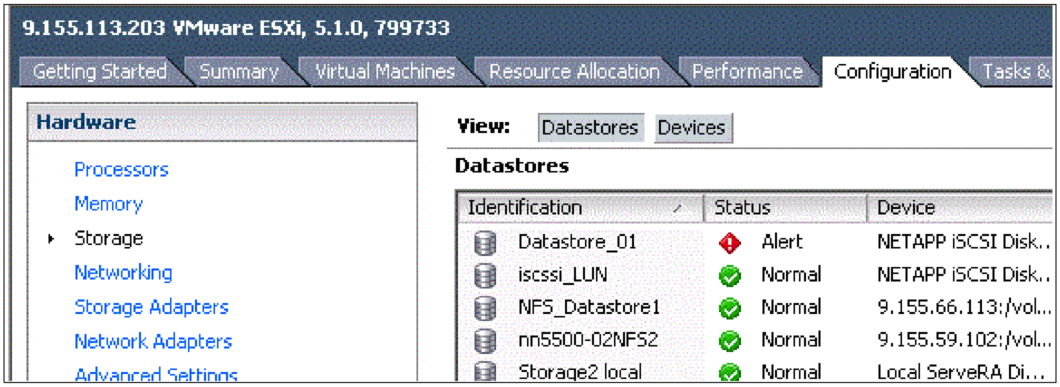
9.155.113.203 VMware ESXi, 5.1.0, 799733

Datastores

Identification	Status	Device
Datastore_01	◆ Alert	NETAPP iSCSI Disk...
iscsi_LUN	✓ Normal	NETAPP iSCSI Disk...
NFS_Datastore1	✓ Normal	9.155.66.113:/vol...
nn5500-02NFS2	✓ Normal	9.155.59.102:/vol...
snap-33c2f85b-D...	◆ *Alert*	*NETAPP iSCSI D...*
Storage2 local	✓ Normal	Local ServeRA Di...

Figure 10-30 Datastore grayed due to LUN unavailability

7. Click **Rescan All...** to remove that datastore from the list, as shown in Figure 10-31.



Identification	Status	Device
Datastore_01	Alert	NETAPP iSCSI Disk..
iscssi_LUN	Normal	NETAPP iSCSI Disk..
NFS_Datastore1	Normal	9.155.66.113:/vol...
nn5500-02NFS2	Normal	9.155.59.102:/vol...
Storage2 local	Normal	Local ServeRA Di...

Figure 10-31 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 feature 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 off-hours backup window, because backups do not impact the primary system, as explained in this chapter. It includes the following topics:

- Licensing the SnapVault locations
- Setting up the primary storage
- Creating a qtree
- Setting up auxiliary storage
- Configuring SnapVault
- Tape backups from the SnapVault secondary system
- Restoring SnapVault snapshots

© Copyright IBM Corp. 2013. All rights reserved.

11.1 Licensing the SnapVault locations

To use SnapVault, you must license the primary (the one from where data will be replicated) and secondary (the one receiving that data) SnapVault locations.

To license the SnapVault locations, perform the following steps:

1. From N series System Manager, navigate to **Configuration** → **System Tools** → **Licenses**, and click **Add**. Type your license and click **Add**, then you should receive a message stating that the license was installed successfully,
2. Repeat these steps on the secondary system, entering the license details into the SnapVault ONTAP Secondary field.

> **Tip:** Primary and Secondary licenses are different in their purpose, so you cannot use a primary license on different storages to establish data replication between them.

11.2 Setting up the primary storage

When setting up a new environment, you can plan your primary storage allocation based upon the backup schedule that you require. Where possible, co-locate data with similar backup requirements sharing the same volumes. For example, make sure that your transient data is stored on separate volumes from your vital data.

The steps for setting up primary storage are similar to setting up any N series storage for Virtual Infrastructure 5. The difference is that storage that has 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. To create a qtree, perform the following steps:

1. From N series System Manager, navigate to **Storage** → **Qtrees** (Figure 11-1).

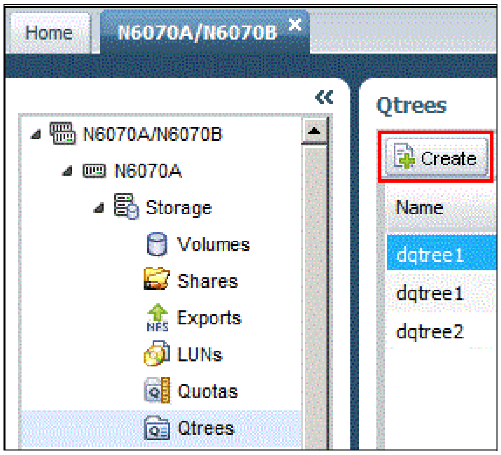
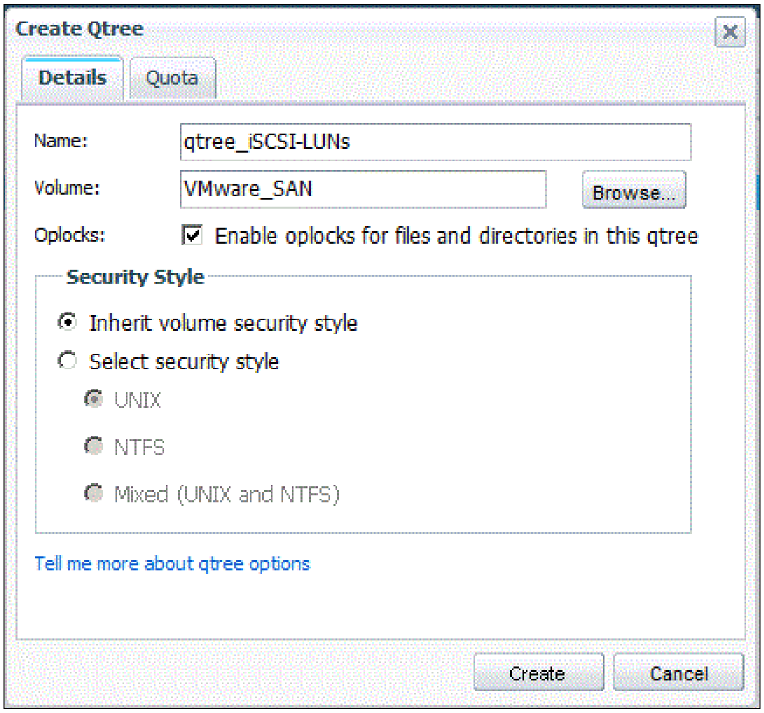


Figure 11-1 Adding a qtree

2. Type a name for the qtree and browse to select the volume to be replicated (Figure 11-2), and click **Create**.



Create Qtree

Details | Quota

Name: qtree_iSCSI-LUNs

Volume: VMware_SAN [Browse...]

Oplocks: ☑ Enable oplocks for files and directories in this qtree

Security Style

● Inherit volume security style

○ Select security style

● UNIX

○ NTFS

○ Mixed (UNIX and NTFS)

Tell me more about qtree options

[Create] [Cancel]

Figure 11-2 qtree properties

3. If the qtree was created successfully, it will display on the qtree list, as shown in Figure 11-3.

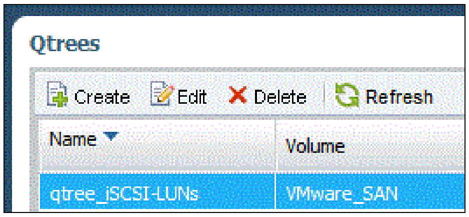


Figure 11-3 qtree created

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>`

   If creating a LUN using IBM N series System Manager, browse to the qtree instead of the volume, as shown in Figure 11-4.

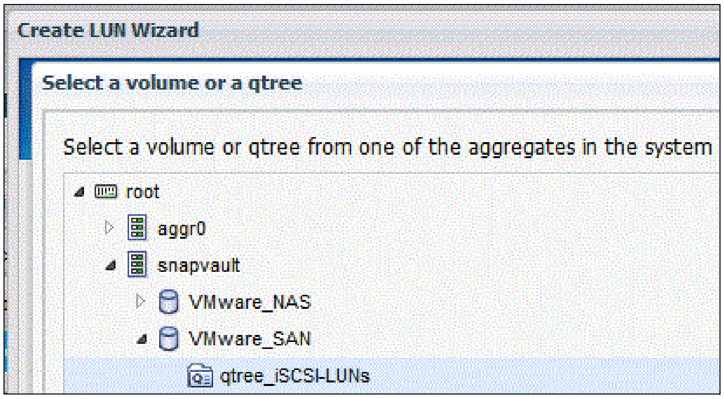

Create LUN Wizard
Select a volume or a qtree
Select a volume or qtree from one of the aggregates in the system
root
aggr0
snapvault
VMware_NAS
VMware_SAN
qtree_iSCSI-LUNs

Figure 11-4 Creating a LUN in the qtree

5. If your LUN exists in the volume, change its path to the qtree. This process has to be done by command-line, using the **lun move** command, as shown in Example 11-1

Example 11-1 The lun move command

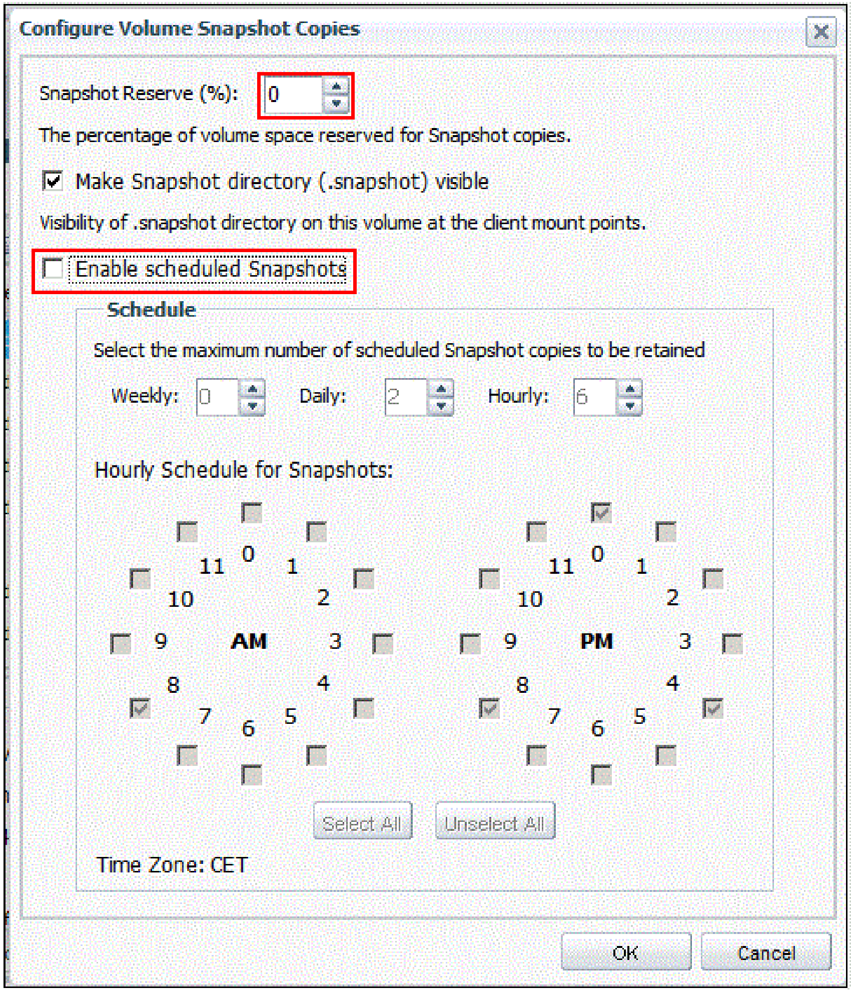
```
N6070A> lun show
        /vol/VMware_SAN/iSCSI_LUN01 150g (161061273600)  (r/w, online, mapped)

N6070A> lun move /vol/VMware_SAN/iSCSI_LUN01
/vol/VMware_SAN/qtree_iSCSI-LUNs/iSCSI_LUN01

N6070A> lun show
        /vol/VMware_SAN/qtree_iSCSI-LUNs/iSCSI_LUN01    150g (161061273600)
(r/w, online, mapped)
```

11.4 Setting up auxiliary storage

After the primary storage configuration, the auxiliary storage has to be set up, which is where the backups will 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** policy on the volume to 0.

To set up auxiliary storage, implement the following steps:

1. Disable Scheduled Snapshots on the secondary filer, as SnapVault will be used to back up data. select the **Storage** →**Volumes**, then select the volume, click **Snapshot** →**Configure.**
2. In the Configure Snapshots pane (Figure 11-5), select the secondary volume that you just created. For Scheduled Snapshots, clear the **Scheduled** check box.



Configure Volume Snapshot Copies

Snapshot Reserve (%): 0

The percentage of volume space reserved for Snapshot copies.

☑ Make Snapshot directory (.snapshot) visible

Visibility of .snapshot directory on this volume at the client mount points.

□ Enable scheduled Snapshots

Schedule

Select the maximum number of scheduled Snapshot copies to be retained

Weekly: 0 Daily: 2 Hourly: 6

Hourly Schedule for Snapshots:

Time Zone: CET

Figure 11-5 Disabling Snapshot schedule

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 Setting permissions

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.

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 11-2):

```
options snapvault.access host=<secondary>
```

Example 11-2 Setting SnapVault permissions

```
N6070A> options snapvault.access host=9.155.66.103
N6070A>
```

Enter the same command on the secondary system, specifying the primary as the host, as shown in Example 11-3:

```
options snapvault.access host=<primary>
```

Example 11-3

```
N6070B> options snapvault.access host=9.155.66.113
N6070B>
```

This configuration allows the primary system to perform restore operations from the secondary system later.

11.5.2 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 11-4):

   ```
   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 11-4 Initial SnapVault

   ```
   N6070B> snapvault start -S 9.155.66.113:/vol/VMware_SAN/qtree_iSCSI-LUNs
   N6070B:/vol/vol_snap/qtree_iSCSI-LUNs-B

   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 11-5).

Example 11-5 Checking the SnapVault Status: Initial SnapVault in progress

```
N6070B> snapvault status
Snapvault secondary is ON.
Source                                        Destination
        State          Lag        Status
9.155.66.113:/vol/VMware_SAN/qtree_iSCSI-LUNs  N6070B:/vol/vol_snap/qtree_iSCSI-
LUNs-B  Uninitialized  -          Transferring  (12 GB done)
```

After the initial SnapVault is complete, the **snapvault status** command is displayed as *idle* (Example 11-6).

Example 11-6 Check SnapVault Status - Initial SnapVault complete

```
N6070B> snapvault status
Snapvault secondary is ON.

Source                                        Destination
        State          Lag        Status
9.155.66.113:/vol/VMware_SAN/qtree_iSCSI-LUNs  N6070B:/vol/vol_snap/qtree_iSCSI-
LUNs-B  Snapvaulted    00:11:43   Idle
N6070B>
```

3. Check the volumes on the secondary system 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.

11.5.3 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 typing the following command on it:

```
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 11-7 shows the command and resulting output for this configuration.

Example 11-7 Scheduling SnapVault snapshots on the primary system

```
N6070A> snapvault snap sched VMware_SAN 8_hourly 6@0,8,16
N6070A> snapvault snap sched
create VMware_SAN 8_hourly 6@0,8,16
```

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 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 11-8 shows the command and resulting output in this situation.

Example 11-8 Scheduling SnapVault snapshot transfers on the secondary system

```
N6070B> snapvault snap sched -x vol_snap 8_hourly 21@0,8,16
N6070B> snapvault snap sched
xfer   vol_snap 8_hourly 21@0,8,16 preserve=default,warn=0
N6070B>
```

11.6 Tape 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.

11.7.1 Preparation

If not configured already, set the permissions on the secondary storage to allow the primary to perform the restore by entering the following command on the secondary system (Example 11-2 on page 188):

```
options snapvault.access host=<primary>
```

Before recovering SnapVault snapshots to Virtual Infrastructure 4.x, the ESXi 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. Enter the following command (Example 11-9) on 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 11-9 SnapVault restore command

```
N6070A> snapvault restore -S 9.155.66.103:/vol/vol_snap/qtree_iSCSI-LUNs-B
N6070A:/vol/VMware_SAN/qtree_restore
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
N6070A>
```

The CLI of 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 11-10.

Example 11-10 SnapVault status: Restore underway

```
N6070B> snapvault status
Snapvault secondary is ON.
Source                                          Destination
        State          Lag        Status
9.155.66.113:/vol/VMware_SAN/qtree_iSCSI-LUNs  N6070B:/vol/vol_snap/qtree_iSCSI-
LUNs-B  Snapvaulted    01:18:05   Idle
N6070B:/vol/vol_snap/qtree_iSCSI-LUNs-B        N6070A:/vol/VMware_SAN/qtree_rest
ore     Source         -          Transferring  (321 MB done)
N6070B>
```

As with the initial snapshot, the restore might take some time, depending on how much data in the qtree has to be restored. When it is completed, the primary CLI shows a success message and becomes available again (Example 11-11).

Example 11-11 Successful restore

```
N6070A> Wed Nov 14 23:47:42 CET [N6070A:vdisk.qtreeRestoreComplete:info]: Qtree
restore is complete for /vol/VMware_SAN/qtree_restore.
```

11.7.3 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 Chapter 7, “Presenting N series storage for VMware vSphere 5.1” on page 99 to map the LUNs.

11.7.4 Mounting a restored image in the VMware host

After the LUN is mapped, rescan the adapters on the VMware hosts. 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 to an existing datastore:

  a. Open the original and restored datastores in vCenter.
  b. Copy the required guest folders from the restored datastore into 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 5.1 and N series storage in the same environment. It then explains the implementation of disaster recovery using the functions of these technologies. It includes the following topics:

- High availability
- Disaster recovery options
- Setting up disaster recovery
- Recovering from a disaster
- Returning to production
- Disaster recovery testing

© Copyright IBM Corp. 2013. All rights reserved.

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.

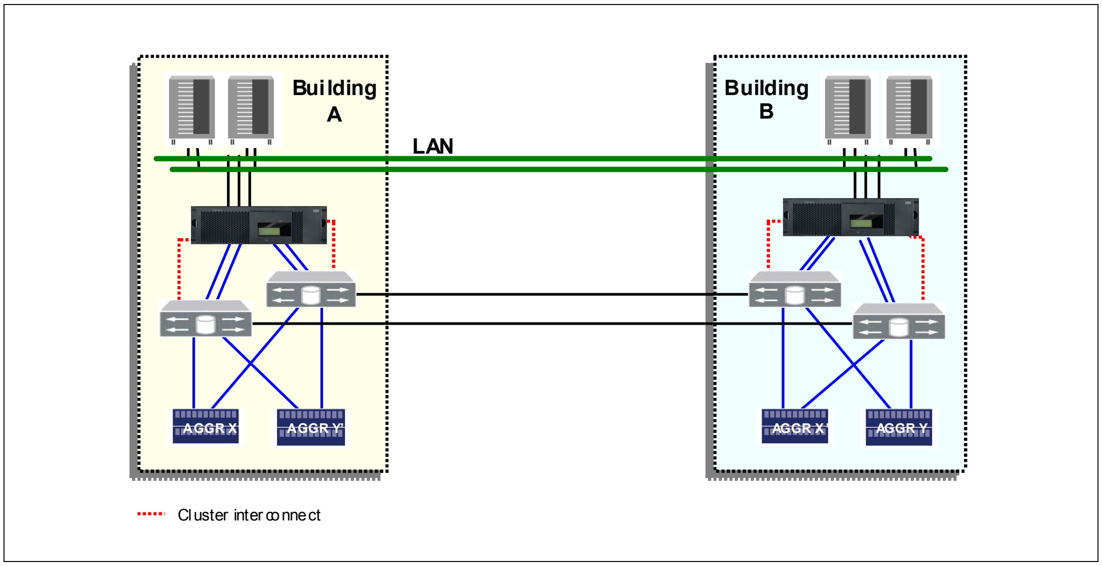


Figure 12-1 MetroCluster configurations

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.

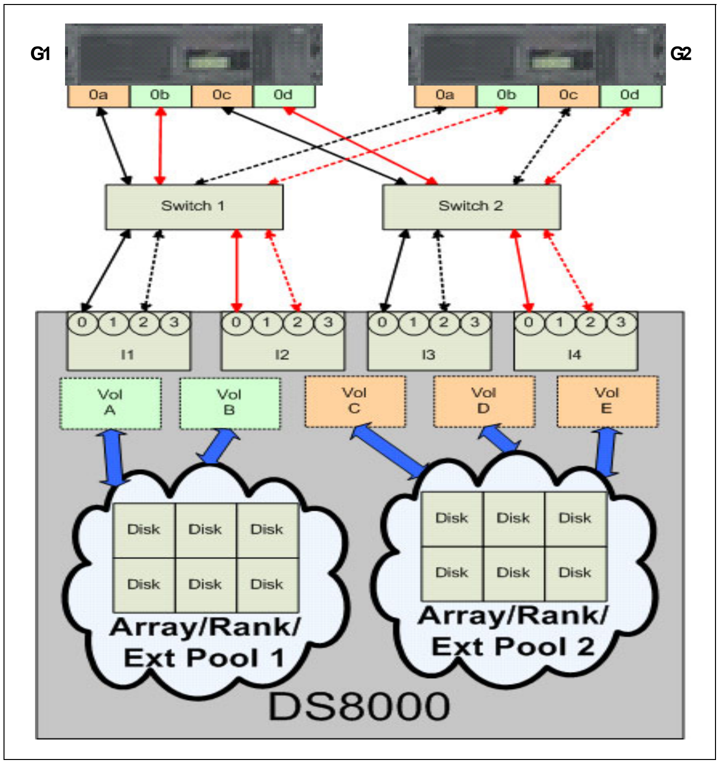


Figure 12-2 N series Gateway cluster configuration

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.

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

   ```
   N6070A> vol restrict vol_vm_dr
   Volume 'vol_vm_dr' is now restricted.
   N6070A>
   ```

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 N series System Manager, in the left navigation pane, select **Configuration** → **System Tools** → **Licenses**.
2. In the Licenses pane (Figure 12-3), click **Add** enter your license code and select **Apply**.

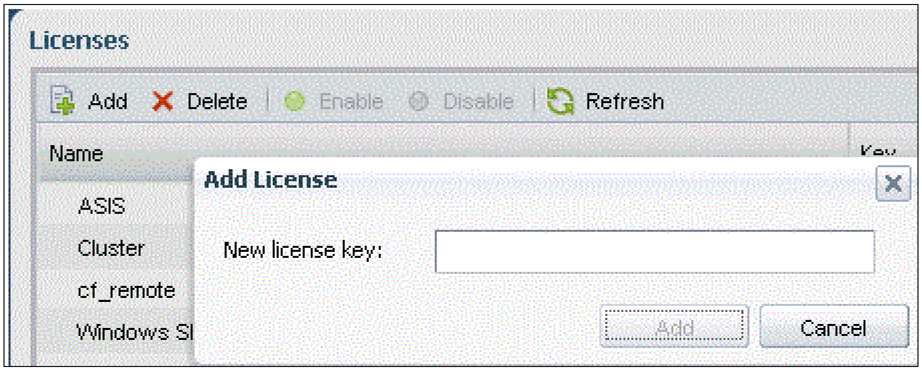


Figure 12-3 SnapMirror License installed

When installed, the SnapMirror options become available in the left navigation pane (Figure 12-4).

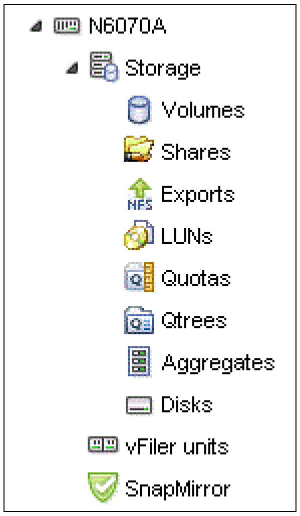


Figure 12-4 SnapMirror menu options

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

```
N6070A> options snapmirror.access host=9.155.66.103
N6070A> options snapmirror.access
snapmirror.access            host=9.155.66.103
N6070A>
```

The **`options snapmirror.access`** command verifies that the permission was assigned correctly.

You can also use this function in System Manager. 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 System Manager, in the left navigation pane (Figure 12-5), select **SnapMirror** → in the right pane, select **Create**.

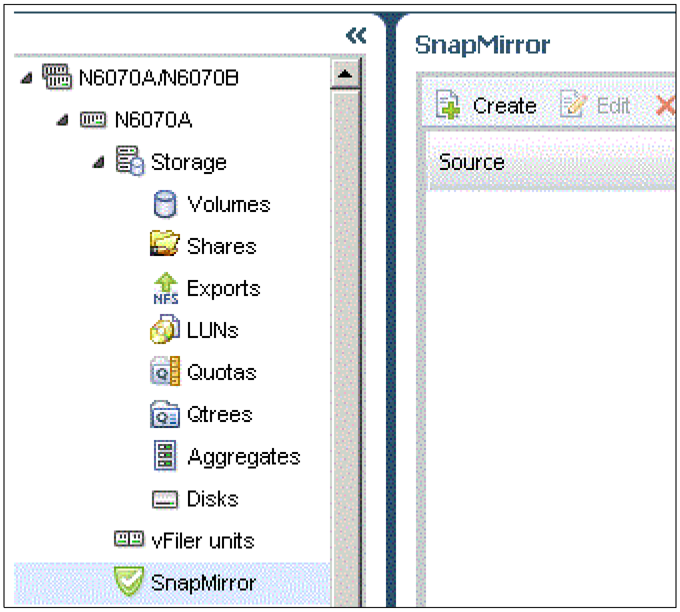
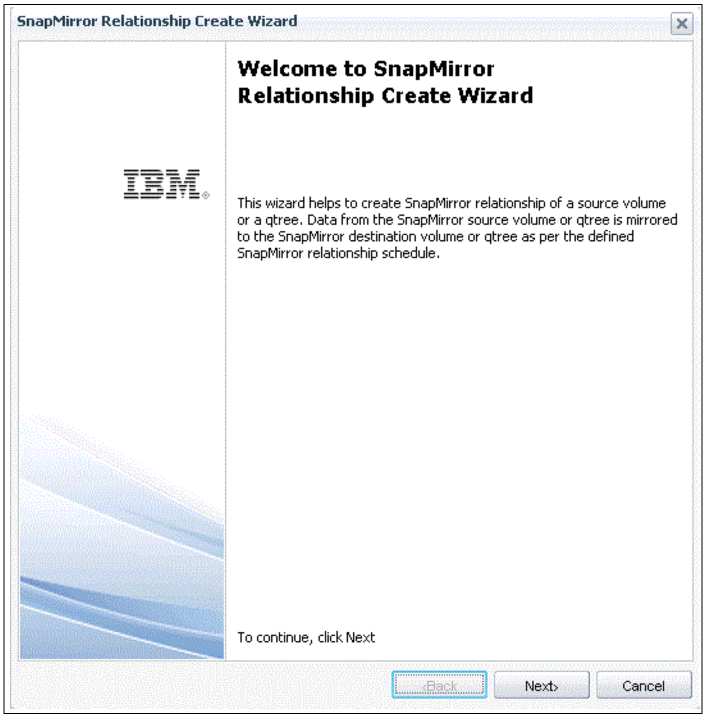


Figure 12-5 Selecting the option to add SnapMirror

2. In the SnapMirror Wizard Welcome panel, click **Next** (Figure 12-6).



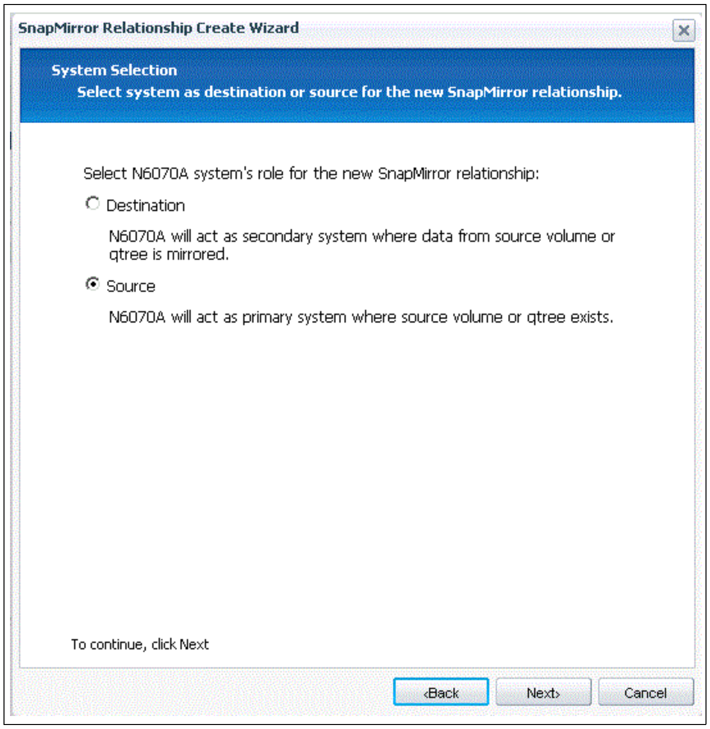
Welcome to SnapMirror Relationship Create Wizard

This wizard helps to create SnapMirror relationship of a source volume or a qtree. Data from the SnapMirror source volume or qtree is mirrored to the SnapMirror destination volume or qtree as per the defined SnapMirror relationship schedule.

To continue, click Next

Figure 12-6 SnapMirror welcome panel

3. In the next panel, you need to select the current host as Source or Destination as shown in Figure 12-7. In this example, the N series N6070A will be used as source. Select **Source** then click **Next**.



SnapMirror Relationship Create Wizard

System Selection
Select system as destination or source for the new SnapMirror relationship.

Select N6070A system's role for the new SnapMirror relationship:

○ Destination

N6070A will act as secondary system where data from source volume or qtree is mirrored.

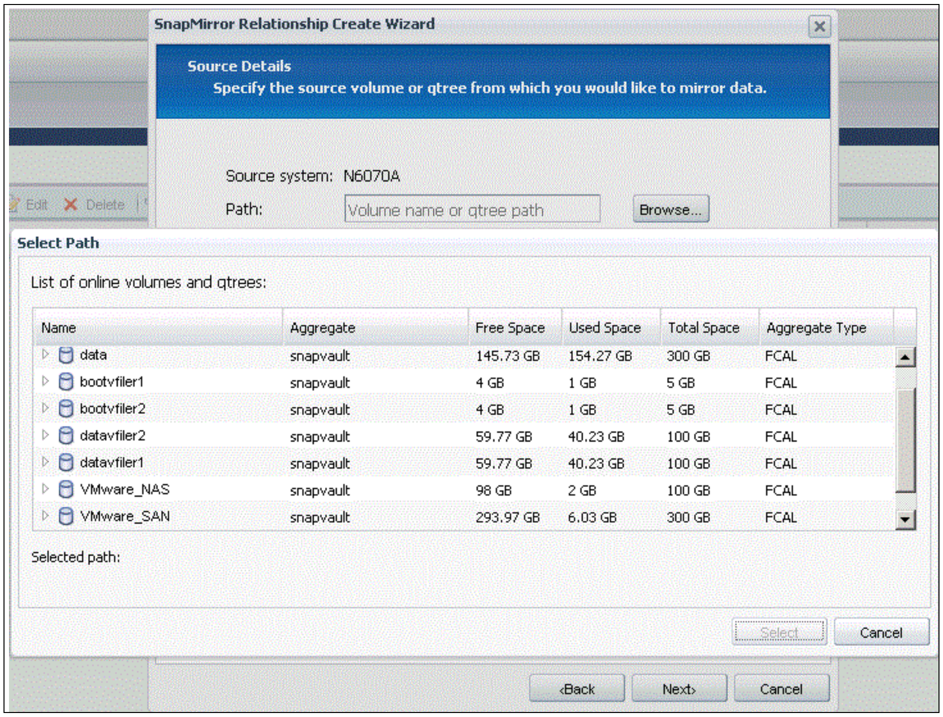
● Source

N6070A will act as primary system where source volume or qtree exists.

To continue, click Next

Figure 12-7 SnapMirror system selection

4. In the Source Selection panel, select the Volume name or qtree path to be mirrored. (Figure 12-8). You can type the path or navigate using browse. Then click **Next**.



SnapMirror Relationship Create Wizard

Source Details
Specify the source volume or qtree from which you would like to mirror data.

Source system: N6070A

Path: Volume name or qtree path

Select Path

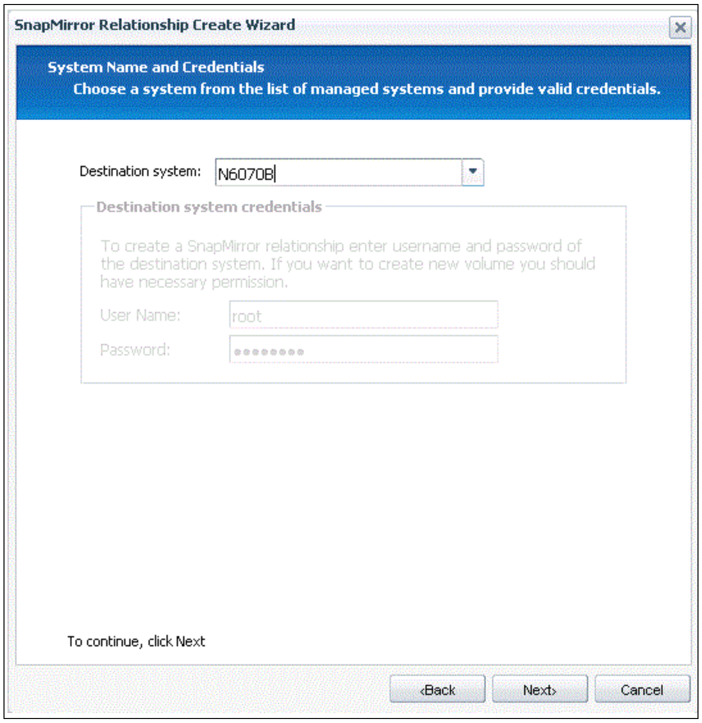
List of online volumes and qtrees:

Name	Aggregate	Free Space	Used Space	Total Space	Aggregate Type
data	snapvault	145.73 GB	154.27 GB	300 GB	FCAL
bootvfiler1	snapvault	4 GB	1 GB	5 GB	FCAL
bootvfiler2	snapvault	4 GB	1 GB	5 GB	FCAL
datavfiler2	snapvault	59.77 GB	40.23 GB	100 GB	FCAL
datavfiler1	snapvault	59.77 GB	40.23 GB	100 GB	FCAL
VMware_NAS	snapvault	98 GB	2 GB	100 GB	FCAL
VMware_SAN	snapvault	293.97 GB	6.03 GB	300 GB	FCAL

Selected path:

Figure 12-8 Browse source path

5. In the next panel, select the Destination System where the volume will the mirrored (Figure 12-9). Then click **Next**.



SnapMirror Relationship Create Wizard

System Name and Credentials

Choose a system from the list of managed systems and provide valid credentials.

Destination system: N6070B

Destination system credentials

To create a SnapMirror relationship enter username and password of the destination system. If you want to create new volume you should have necessary permission.

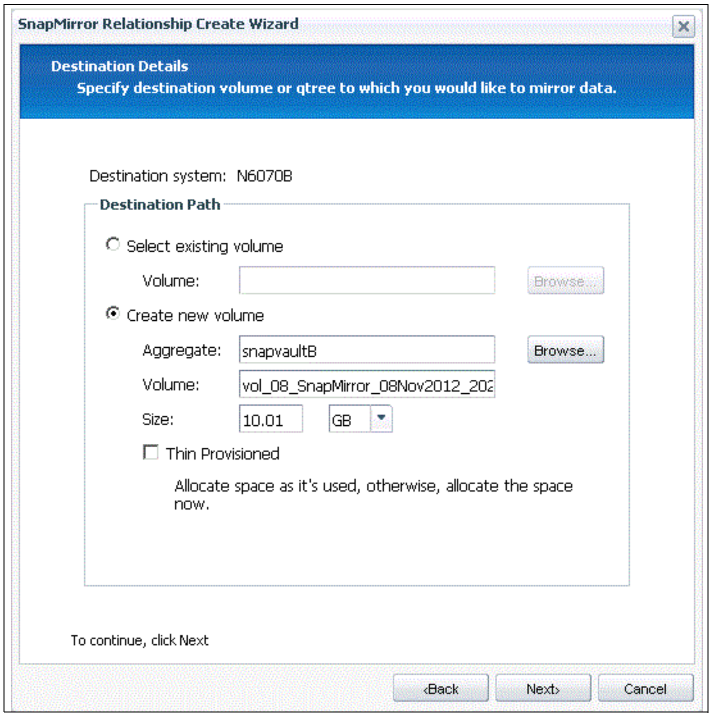
User Name: root

Password: ●●●●●●●●

To continue, click Next

Figure 12-9 Select destination system

6. In the next panel, select the destination path for the mirrored volume. You can create a new volume or select an existing. The volume must be in restricted mode in the second case. We are going to create a new volume (Figure 12-10). Then click **Next**.



SnapMirror Relationship Create Wizard

Destination Details

Specify destination volume or qtree to which you would like to mirror data.

Destination system: N6070B

Destination Path

○ Select existing volume

Volume:

● Create new volume

Aggregate: snapvaultB

Volume: vol_08_SnapMirror_08Nov2012_202

Size: 10.01 GB

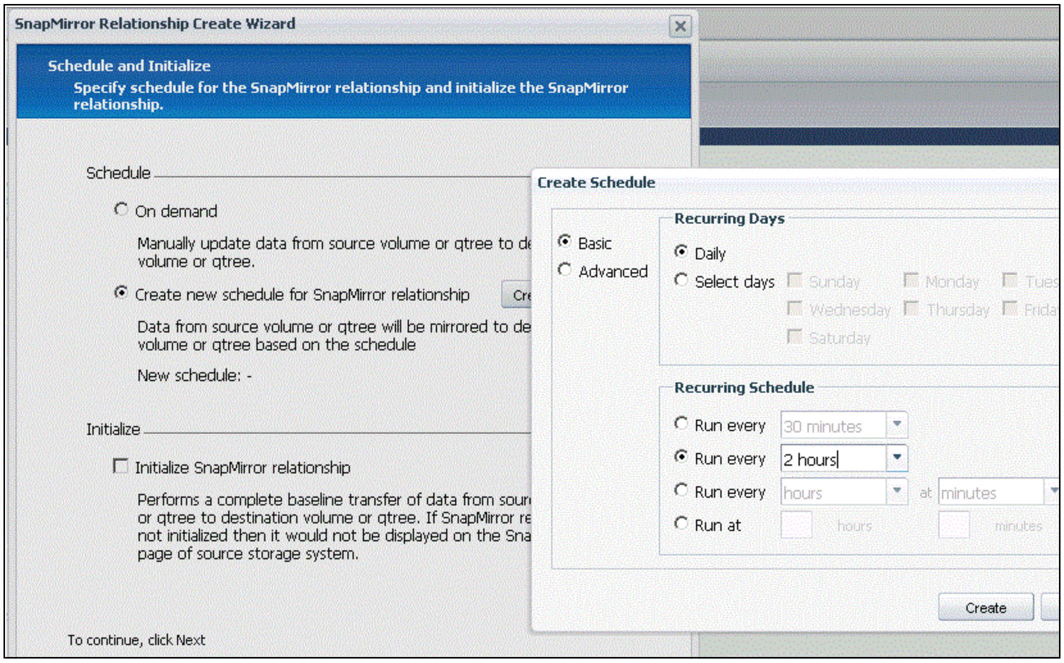
□ Thin Provisioned

Allocate space as it's used, otherwise, allocate the space now.

To continue, click Next

Figure 12-10 Select the destination path

7. In the Schedule and Initialize panel, you can create a schedule for the SnapMirror relationship or just leave On demand. We are going to create a basic schedule. Select the *Create new schedule for SnapMirror relationship* option and click **Create** (Figure 12-11).



SnapMirror Relationship Create Wizard

Schedule and Initialize

Specify schedule for the SnapMirror relationship and initialize the SnapMirror relationship.

Schedule

○ On demand

Manually update data from source volume or qtree to de volume or qtree.

● Create new schedule for SnapMirror relationship

Data from source volume or qtree will be mirrored to de volume or qtree based on the schedule

New schedule: -

Initialize

□ Initialize SnapMirror relationship

Performs a complete baseline transfer of data from sour or qtree to destination volume or qtree. If SnapMirror re not initialized then it would not be displayed on the Sna page of source storage system.

To continue, click Next

Create Schedule

● Basic

○ Advanced

Recurring Days

● Daily

○ Select days □ Sunday □ Monday □ Tues □ Wednesday □ Thursday □ Frida □ Saturday

Recurring Schedule

○ Run every 30 minutes

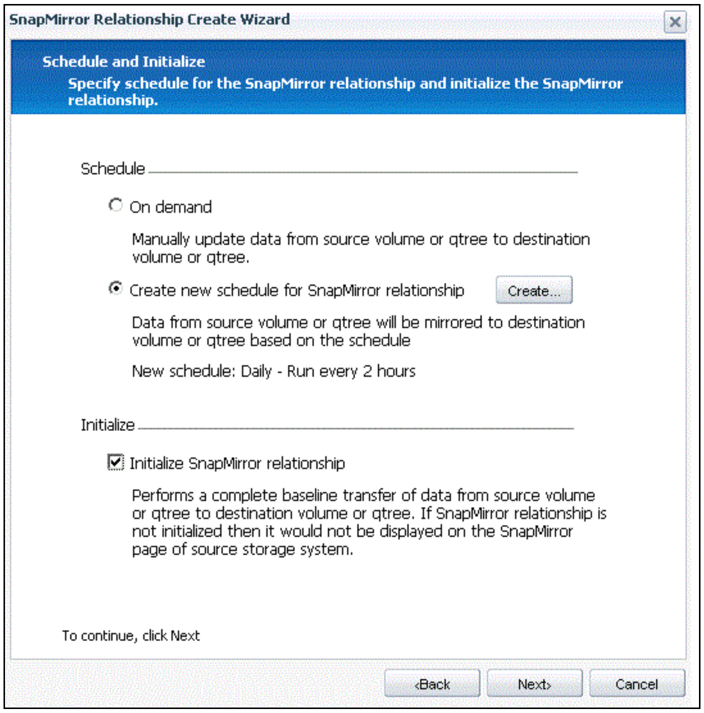
● Run every 2 hours

○ Run every hours at minutes

○ Run at hours minutes

Figure 12-11 Create SnapMirror schedule

8. Still in the Schedule and Initialize panel (Figure 12-12), after you configure the mirror, you must initialize it to start the initial mirror copy to the destination storage system. Select the Initialize SnapMirror relationship check box and click **Next**.



SnapMirror Relationship Create Wizard

Schedule and Initialize

Specify schedule for the SnapMirror relationship and initialize the SnapMirror relationship.

Schedule

○ On demand

Manually update data from source volume or qtree to destination volume or qtree.

● Create new schedule for SnapMirror relationship

Data from source volume or qtree will be mirrored to destination volume or qtree based on the schedule

New schedule: Daily - Run every 2 hours

Initialize

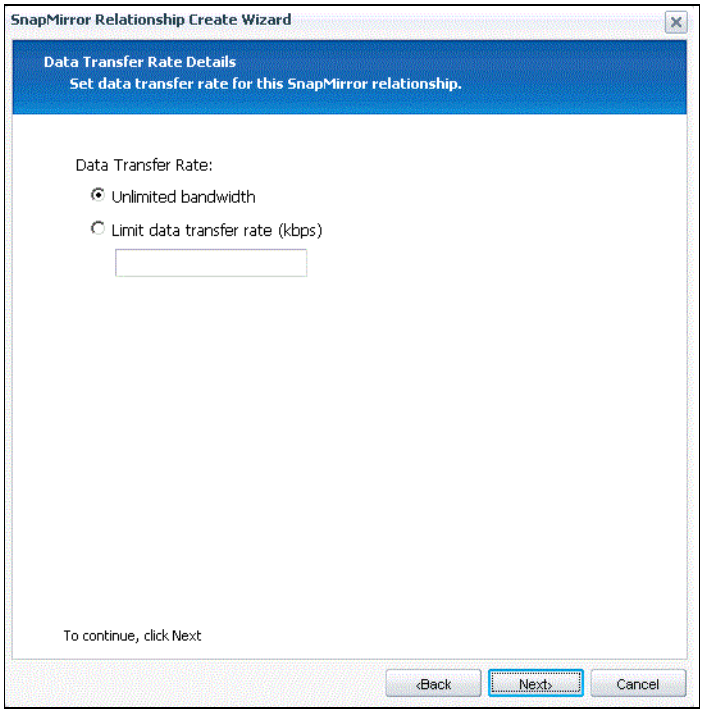
☑ Initialize SnapMirror relationship

Performs a complete baseline transfer of data from source volume or qtree to destination volume or qtree. If SnapMirror relationship is not initialized then it would not be displayed on the SnapMirror page of source storage system.

To continue, click Next

Figure 12-12 Initialize SnapMirror

9. In the next wizard panel (Figure 12-13), you can select how much bandwidth you want reserve for the SnapMirror. Leave it unlimited unless you experience any network performance issues after the creation. Click **Next**.



SnapMirror Relationship Create Wizard

Data Transfer Rate Details
Set data transfer rate for this SnapMirror relationship.

Data Transfer Rate:

● Unlimited bandwidth

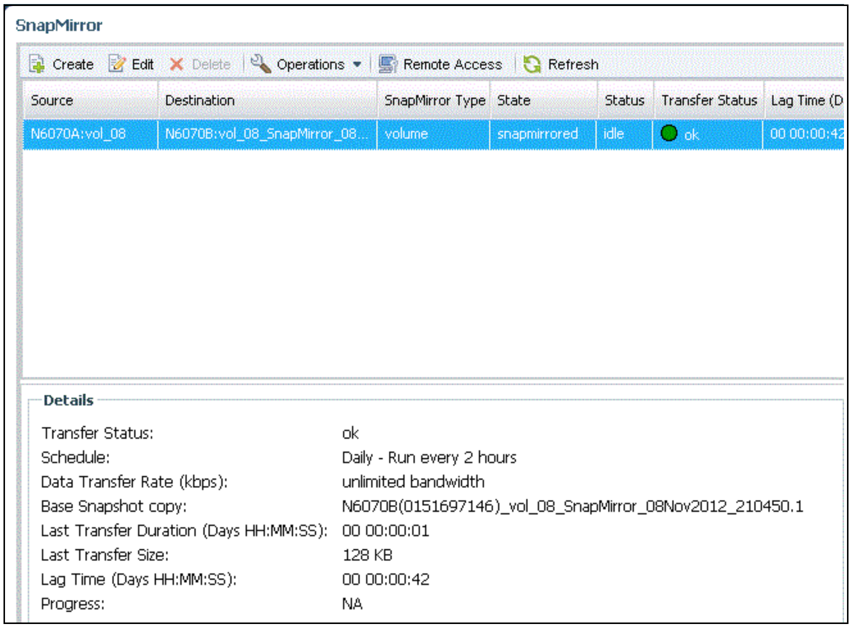
○ Limit data transfer rate (kbps)

To continue, click Next

Figure 12-13 Select bandwidth

10. The next panel is the SnapMirror Relationship summary. Review and click **Next**.

11. Verify the SnapMirror status by selecting SnapMirror in the System Manager left pane as shown in Figure 12-14.



SnapMirror

Source	Destination	SnapMirror Type	State	Status	Transfer Status	Lag Time (D
N6070A:vol_08	N6070B:vol_08_SnapMirror_08...	volume	snapmirrored	idle	● ok	00 00:00:42

Details

Transfer Status:	ok
Schedule:	Daily - Run every 2 hours
Data Transfer Rate (kbps):	unlimited bandwidth
Base Snapshot copy:	N6070B(0151697146)_vol_08_SnapMirror_08Nov2012_210450.1
Last Transfer Duration (Days HH:MM:SS):	00 00:00:01
Last Transfer Size:	128 KB
Lag Time (Days HH:MM:SS):	00 00:00:42
Progress:	NA

Figure 12-14 SnapMirror status

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 System Manager on the destination N series system.
2. In the left navigation pane of System Manager (Figure 12-15), select **SnapMirror** → Highlight the desired SnapMirror relationship → **Operations** → **Break**.

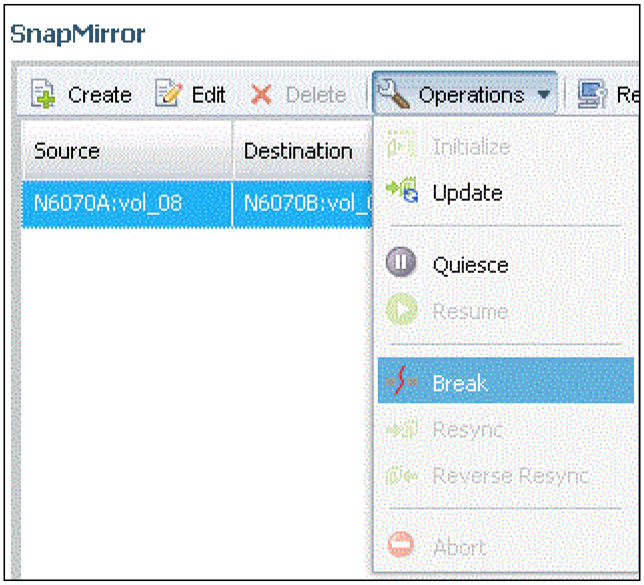
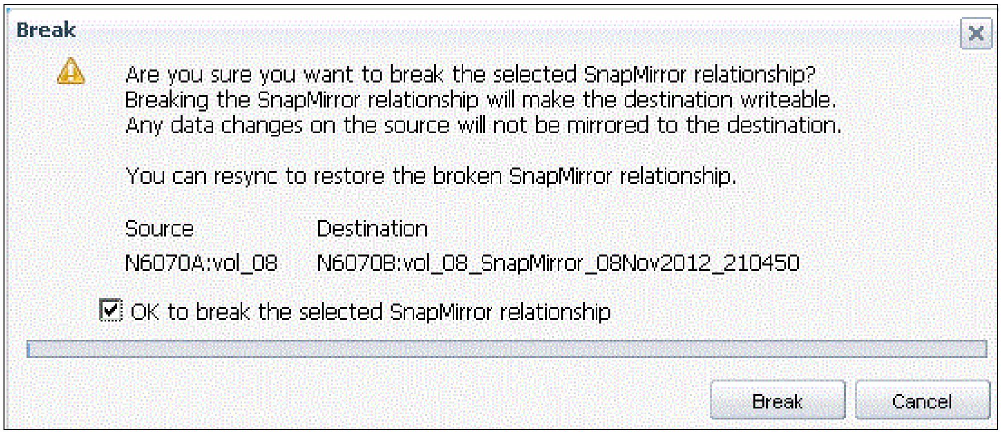


Figure 12-15 Break SnapMirror

3. In the SnapMirror Break confirmation panel (Figure 12-16), select **OK to break the selected SnapMirror relationship** and click **Break**.



Break

Are you sure you want to break the selected SnapMirror relationship?
Breaking the SnapMirror relationship will make the destination writeable.
Any data changes on the source will not be mirrored to the destination.

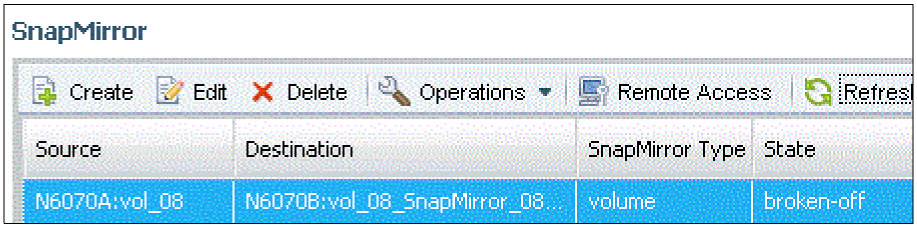
You can resync to restore the broken SnapMirror relationship.

Source	Destination
N6070A:vol_08	N6070B:vol_08_SnapMirror_08Nov2012_210450

☑ OK to break the selected SnapMirror relationship

Figure 12-16 Confirm SnapMirror break

4. In the SnapMirror pane (Figure 12-17), you can see that the mirror was broken.



SnapMirror

Source	Destination	SnapMirror Type	State
N6070A:vol_08	N6070B:vol_08_SnapMirror_08...	volume	broken-off

Figure 12-17 Broken SnapMirror

5. 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.

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. Verify the task list to confirm that the guest started correctly.
3. 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.

> **GUI versus CLI commands:** It is possible to perform some of the steps in this section and the following sections from System Manager. 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 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>
```

Figure 12-18 shows how to perform the same operation using the System Manager console.

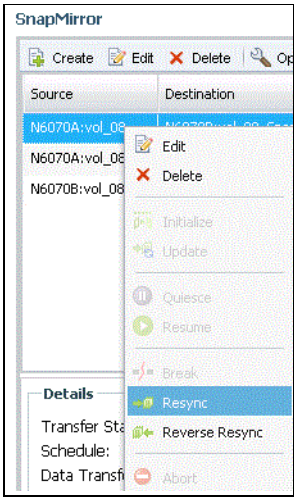


Figure 12-18 Resync SnapMirror

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 12-3 shows the `snapmirror initialize` command.

Example 12-3 Copying the disaster recovery environment data to the production site

```
N6070A> snapmirror initialize -S 9.155.66.103:vol_08_SnapMirror_08Nov2012_210450
N6070A:vol_08
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 12-4 shows the results of the **snapmirror update** command.

Example 12-4 Updating data between the disaster recovery and production sites

```
N6070A> snapmirror update -S 9.155.66.103:vol_08_SnapMirror_08Nov2012_210450
N6070A:vol_08
Transfer started.
Monitor progress with 'snapmirror status' or the snapmirror log.
N6070A>
```

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 12-5 shows the execution of the **snapmirror break** command.

Example 12-5 Breaking the mirror

```
N6070A> snapmirror break vol_08
snapmirror break: Destination vol_08 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.
N6070A>
```

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 12-6 shows the results of the **snapmirror resync** command.

Example 12-6 Resync from the production to disaster recovery site

```
N6070A> snapmirror resync vol_08_SnapMirror_08Nov2012_210450
The resync base Snapshot will be:
N6070B(0151697146)_vol_08_SnapMirror_08Nov2012_210450.2
Are you sure you want to resync the volume? yes
Thu Nov 9 16:32:15 CET [snapmirror.dst.resync.info:notice]: SnapMirror resync of
vol_08_SnapMirror_08Nov2012_210450 to
9.155.66.103:vol_08_SnapMirror_08Nov2012_210450 is using
N6070B(0151697146)_vol_08_SnapMirror_08Nov2012_210450.2 as the base Snapshot.
Volume vol_08_SnapMirror_08Nov2012_210450 will be briefly unavailable before
coming back online.
Thu Nov  9 16:32:16 CET [wafl.snaprestore.revert:notice]: Reverting volume
vol_08_SnapMirror_08Nov2012_210450 to a previous Snapshot.
Thu Nov  9 16:32:16 CET [wafl.vol.guarantee.replica:info]: Space for replica
volume 'vol_08_SnapMirror_08Nov2012_210450' is not guaranteed.
Revert to resync base Snapshot was successful.
```

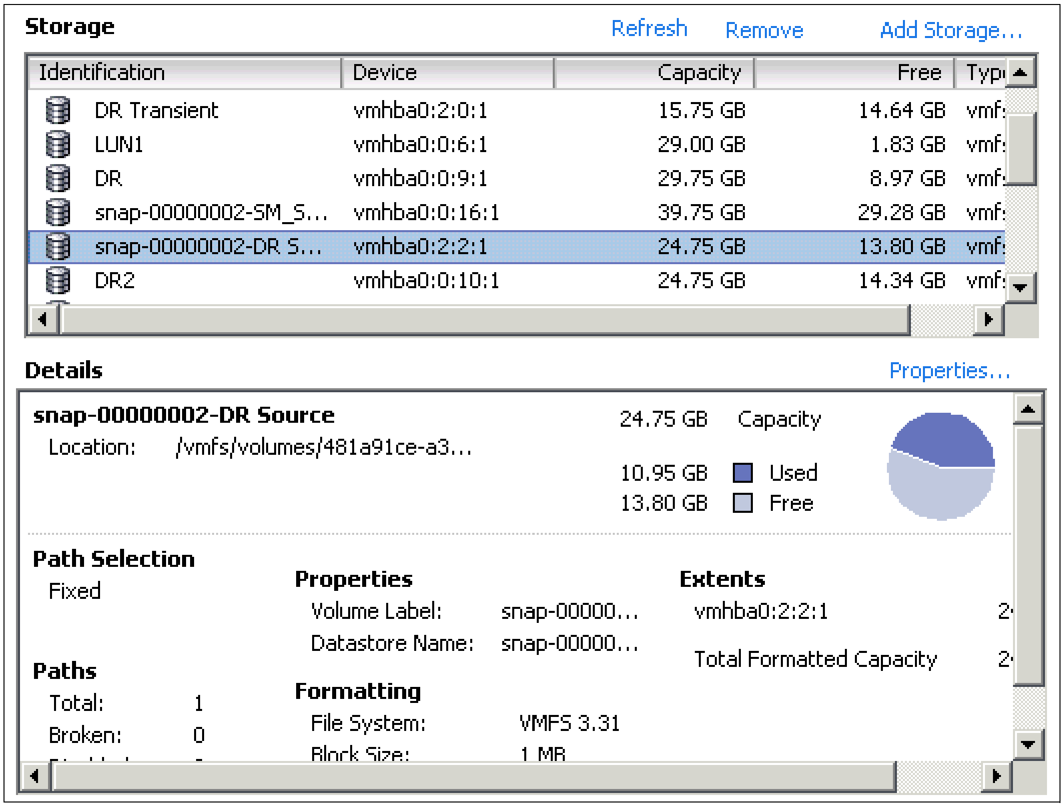
```
Thu Nov  9 16:32:16 CET [snapmirror.dst.resync.success:notice]: SnapMirror resync
of vol_08_SnapMirror_08Nov2012_210450 to
9.155.66.103:vol_08_SnapMirror_08Nov2012_210450 successful.
Transfer started.
Monitor progress with 'snapmirror status' or the snapmirror log.
N6070A>
```

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 shown in Figure 12-19.



Identification	Device	Capacity	Free	Typ
DR Transient	vmhba0:2:0:1	15.75 GB	14.64 GB	vmf:
LUN1	vmhba0:0:6:1	29.00 GB	1.83 GB	vmf:
DR	vmhba0:0:9:1	29.75 GB	8.97 GB	vmf:
snap-00000002-SM_S...	vmhba0:0:16:1	39.75 GB	29.28 GB	vmf:
snap-00000002-DR S...	vmhba0:2:2:1	24.75 GB	13.80 GB	vmf:
DR2	vmhba0:0:10:1	24.75 GB	14.34 GB	vmf:

snap-00000002-DR Source
Location: /vmfs/volumes/481a91ce-a3...

24.75 GB Capacity
10.95 GB ■ Used
13.80 GB □ Free

Path Selection
Fixed

Paths
Total: 1
Broken: 0

Properties
Volume Label: snap-00000...
Datastore Name: snap-00000...

Formatting
File System: VMFS 3.31
Block Size: 1 MB

Extents
vmhba0:2:2:1 2
Total Formatted Capacity 2

Figure 12-19 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 / Compression with VMware vSphere 5.1

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 5.1 environment. It 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

© Copyright IBM Corp. 2013. All rights reserved.

13.1 A-SIS deduplication overview

N series deduplication is a technology that can reduce the physical storage required to store 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.

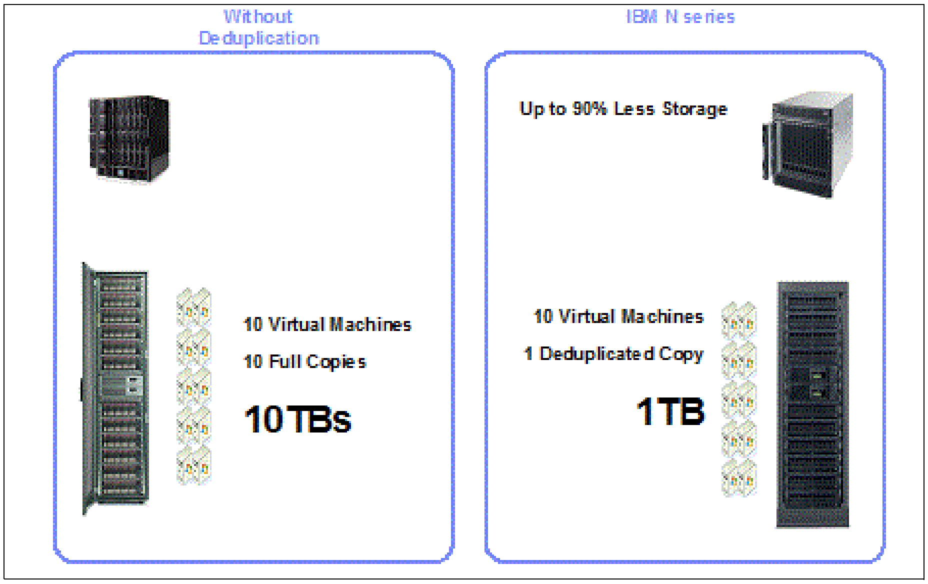


Figure 13-1 A-SIS savings

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 efficiency. During the deduplication process, fingerprints of 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 to 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, thus the performance impact of deduplication is low. It runs on a pre-determined schedule or can be started manually at any time. During times when the storage system is busy or is accepting new write operations, the only impact is the lightweight fingerprinting process. The total impact to performance of the system is imperceptible. 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. 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 a best practice to run it during a period of low activity.

The options to start the deduplication process are flexible, as it can be started automatically on a fixed schedule, after a defined amount of new data was written to the volume (20% by default) or manually started by the administrator at any time.

Consider to run the deduplication process manually when a significant amount of data must be deduplicated, for instance, 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 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, you might want to deduplicate new data before any snapshots are taken.

13.5 Enabling deduplication on a volume

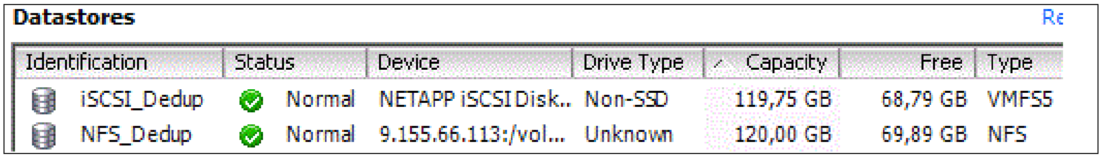
This section explains how to set up deduplication on an N series for use with VMware hosts. It also provides information about storage reduction after enabling it for Network File System (NFS) and iSCSI volumes.

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 iSCSI. The size for the iSCSI LUN and the NFS share is 120 GB each.

The deduplication process

Figure 13-2 shows the original sizes of the NFS and VMFS datastores where the clones are running.



Datastores Re

Identification	Status	Device	Drive Type	Capacity	Free	Type
iSCSI_Dedup	✓ Normal	NETAPP iSCSI Disk...	Non-SSD	119,75 GB	68,79 GB	VMFS5
NFS_Dedup	✓ Normal	9.155.66.113:/vol...	Unknown	120,00 GB	69,89 GB	NFS

Figure 13-2 NFS size on the 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

```
N6070A> df -g /vol/VMWare_NAS
Filesystem               total       used      avail capacity  Mounted on
/vol/VMWare_NAS/         120GB       50GB       69GB      42%  /vol/VMWare_NAS/
/vol/VMWare_NAS/.snapshot        0GB         0GB         0GB     ---%  /vol/VMWare
_NAS/.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

```
N6070A> df -g /vol/LUNdedup
Filesystem               total       used      avail capacity  Mounted on
/vol/LUNdedup/           120GB       50GB       69GB      42%  /vol/LUNdedup/
/vol/LUNdedup/.snapshot        0GB         0GB         0GB     ---%  /vol/LUNdedup
/.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

```
N6070A> sis on /vol/VMWare_NAS
SIS for "/vol/VMWare_NAS" is enabled.
Already existing data could be processed by running "sis start -s /vol/VMWare_NA
S".
```

- 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 /vol/LUNdedup fractional_reserve 0
  ```

b. Enable deduplication on the FCP volume (Example 13-5).

Example 13-5 Enabling deduplication on the FCP volume

```
N6070A> sis on /vol/LUNdedup
SIS for "/vol/LUNdedup" is enabled.
Already existing data could be processed by running "sis start -s
/vol/LUNdedup".
```

c. Check the status (Example 13-6).

Example 13-6 Checking the status

```
N6070A> sis status
Path                           State      Status     Progress
/vol/VMWare_NAS                Enabled    Idle       Idle for 00:50:29
/vol/LUNdedup                  Enabled    Idle       Idle for 00:00:37
```

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, proceed as follows:

To start the deduplication process, use the **`sis start -s <vol_name>`** command (Example 13-7).

Example 13-7 Starting the deduplication process

```
N6070A> sis start -s /vol/VMWare_NAS
The file system will be scanned to process existing data in /vol/VMWare_NAS.
This operation may initialize related existing metafiles.
```

Type **y** when asked to proceed with the scan, and the operation will start (Example 13-8).

Example 13-8 Accepting to proceed with deduplication

```
Are you sure you want to proceed (y/n)? y
The SIS operation for "/vol/VMWare_NAS" is started.
N6070A> Fri Nov 16 00:52:58 CET [N6070A:wafl.scan.start:info]: Starting SIS volu
me scan on volume VMWare_NAS.
```

Example 13-9 shows how to start the deduplication process on a SAN volume, typing **y** when asked to proceed:

Example 13-9 Starting the deduplication process on a SAN volume

```
N6070A> sis start -s /vol/LUNdedup
The file system will be scanned to process existing data in /vol/LUNdedup.
This operation may initialize related existing metafiles.
Are you sure you want to proceed (y/n)? y
The SIS operation for "/vol/LUNdedup" is started.
N6070A> Fri Nov 16 00:57:00 CET [N6070A:wafl.scan.start:info]: Starting SIS volu
me scan on volume LUNdedup.
```

13.5.2 Deduplication results

To check the progress of the deduplication process, use the **`sis status`** command, as shown in Example 13-10. If the status is `active`, the process of deduplication is still on going. If the status is `idle`, deduplication is completed.

Example 13-10 Checking status

```
N6070A> sis status
Path                           State      Status     Progress
/vol/VMWare_NAS                Enabled    Active     47 GB Scanned
/vol/LUNdedup                  Enabled    Active     11 GB Scanned
```

You might see some intermediate results while the deduplication runs, as shown in Example 13-11. Just wait it finishes.

Example 13-11 Intermediate results

```
N6070A> sis status
Path                           State      Status     Progress
/vol/VMWare_NAS                Enabled    Active     5480 MB (11%) Done
/vol/LUNdedup                  Enabled    Active     35 GB Scanned
```

When the process is completed, all volumes will be listed as **`Idle`**, as shown in Example 13-12.

Example 13-12 Process completed

```
N6070A> sis status
Path                           State      Status     Progress
/vol/VMWare_NAS                Enabled    Idle       Idle for 00:07:38
/vol/LUNdedup                  Enabled    Idle       Idle for 00:11:42
```

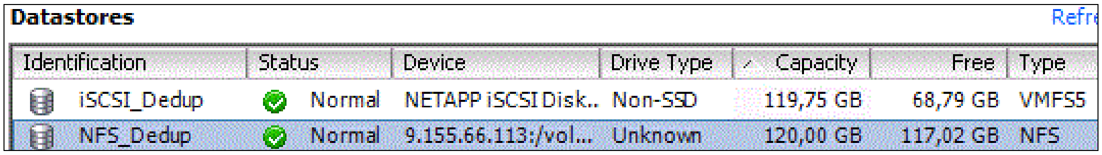
The amount of saved space can be checked you can view the space savings from the vSphere client or on the storage controller. Use the **`df -gs`** command, as shown in Example 13-13.

Example 13-13 N series node

```
N6070A> df -gs /vol/VMWare_NAS
Filesystem                used        saved        %saved
/vol/VMWare_NAS/           2GB         47GB           94%
```

The space savings of NFS volumes are available immediately and can be observed from both the storage controller and vSphere client. The NFS example started with a total of 50 GB being used, 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 ESXi management console. Figure 13-3 shows 117.02 GB of space is available on the NFS share.



Datastores

Identification	Status	Device	Drive Type	Capacity	Free	Type
iSCSI_Dedup	✓ Normal	NETAPP iSCSI Disk..	Non-SSD	119,75 GB	68,79 GB	VMFS5
NFS_Dedup	✓ Normal	9.155.66.113:/vol...	Unknown	120,00 GB	117,02 GB	NFS

Figure 13-3 Savings display

13.5.3 Deduplication of LUNs

Deduplication is effective on both NFS and LUNs. However, as a default behavior, a LUN on the N series storage system reserves its space in the volume where it resides. Deduplication cannot reduce this reservation. To reclaim the space savings, the LUN reservation 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.

After deduplication is complete, you can use the free space gained to store new data, by either creating a LUN in the same volume and connect it as a new datastore, shrinking the existing volume and use the saved space to grow other volumes or creating new volumes.

To disable space reservation for the LUN, run the **`lun set reservation <lun_path>`** command (Example 13-14).

Example 13-14 Setting LUN reservation

```
N6070A> lun set reservation vol/LUNdedup/iSCSI_dedup disable
```

Now the storage savings can be seen as shown in Example 13-15.

Example 13-15 Storage savings displayed

```
N6070A> df -gs /vol/LUNdedup
Filesystem                used      saved       %saved
/vol/LUNdedup/             2GB       48GB          95%
```

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 shown 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.

Unlike NFS, the FCP savings are not apparent when you verify the VMware vCenter management console, as seen in Figure 13-3 on page 216.

14

Virtual Storage Tiering

This chapter explains the features of N series Virtual Storage Tiering. This technology offers the following key benefits:

- Data center efficiency
- Dynamic performance scaling
- Reduced complexity

This chapter includes the following topics:

- Automated storage tiering
- Choosing VST options

© Copyright IBM Corp. 2013. All rights reserved.

14.1 Automated storage tiering

Automated storage tiering (AST) technologies are primarily intended to help data centers benefit from the improved performance of Flash-based media while minimizing cost and complexity. Flash-based devices such as solid-state disk (SSD) controller-based Flash can complete 25 to 100 times more random read operations per second than the fastest hard disk drives (HDDs), but that performance comes at a premium of 15 to 20 times higher cost per gigabyte. HDDs continue to improve in capacity, but HDD performance in terms of IOPS per dollar is relatively stagnant. Flash provides far more IOPS per dollar, plus lower latency.

Figure 14-1 shows a comparison of the random read efficiency of different types of solid-state and rotational media on a logarithmic scale. Note that in terms of IOPS per dollar, there is relatively little difference between different HDD types.

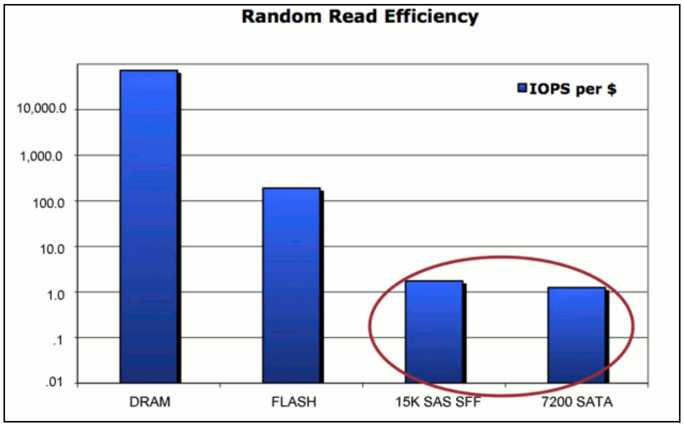


Figure 14-1 Storage efficiency

Rather than permanently placing an entire dataset on expensive media, automated storage tiering tries to identify and store hot data on higher-performance storage media while storing cold data on slower, lower-cost media.

IBM has put a lot of time and energy into understanding the problems that AST must address in order to architect an optimal solution.

There are two fundamentally different approaches to AST: migration and caching, as shown in Figure 14-2.

Migration-based AST automates the process of data migration. When a chunk of data is identified as “hot,” that chunk is moved to faster media and then moved back to slower media when it becomes cold. HDD access is needed both for movement to Flash and movement out of Flash.

Caching-based AST uses well-understood caching methods to “promote” hot data to high-performance media. Because a copy of the data remains on HDD, when data becomes cold it can simply be released from cache with no additional HDD I/O required.

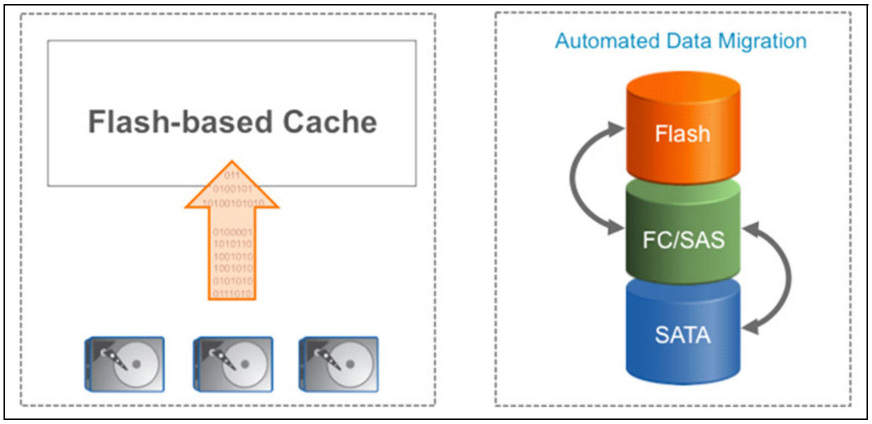


Figure 14-2 Migration versus caching

14.1.1 Traditional and virtual storage tiering

Virtual storage tiering (VST) is performed natively within Data ONTAP and can be extended with the use of Flash Cache. Flash Cache is the hardware component; the software component is called FlexScale.

This section describes these components and the N series best practices to use them in a VMware environment.

Traditional legacy storage arrays

With traditional legacy storage arrays, there is no data or cache deduplication; therefore, for best performance the amount of cache needed should be equal to or greater than the working set size. This leads to requiring either large amounts of cache or more spindles to satisfy peak workloads such as boot, login, or virus storms. Figure 14-3 shows traditional legacy storage array caching.

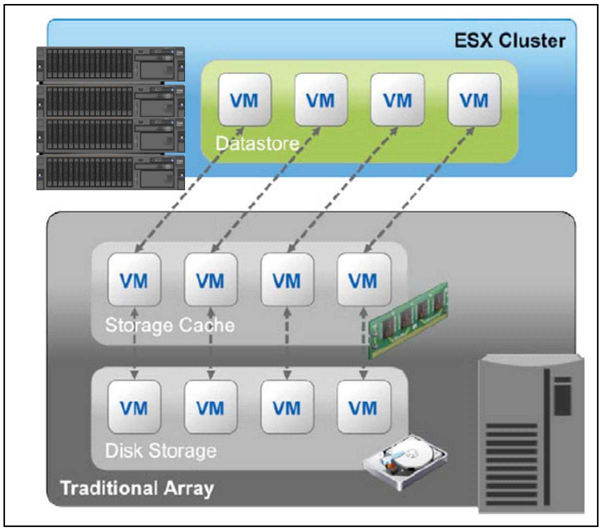


Figure 14-3 Traditional storage tiering

VST in Data ONTAP

Data ONTAP stores only a single block on disk and in cache for up to 255 physical blocks per volume, thus requiring fewer spindles and less cache than legacy storage arrays. Data ONTAP VST is available in all versions of Data ONTAP 7.3.1 or higher. It means that VST can be used in every IBM N series system that supports Data ONTAP 7.3.1 and block-sharing technologies (for example, deduplication and FlexClone volumes). Figure 14-4 shows cache and data deduplication with VST.

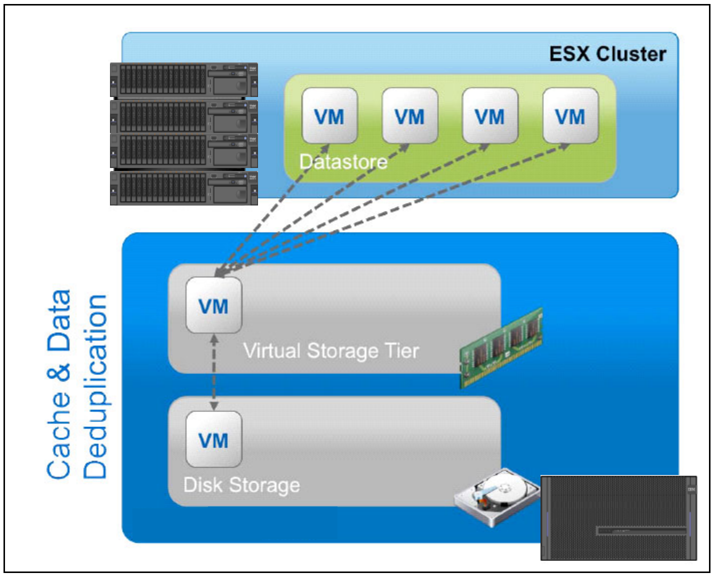


Figure 14-4 Cache and data deduplication

How Data ONTAP VST functions

When a data block is requested, Data ONTAP reads the block into main memory (also known as WAFL buffer cache). If that data block is a deduplicated block, in that it has multiple files referencing the same physical block, each subsequent read of that same physical block comes from cache as long as it has not been evicted from cache. Heavily referenced blocks that are frequently read reside in cache longer than blocks that have fewer references or less frequent access. Therefore, because main memory can be accessed much more quickly than disk, latency is decreased, disk utilization is decreased, and network throughput is increased, thus improving overall performance and end-user experience. Figure 14-5 shows VST with data deduplication.

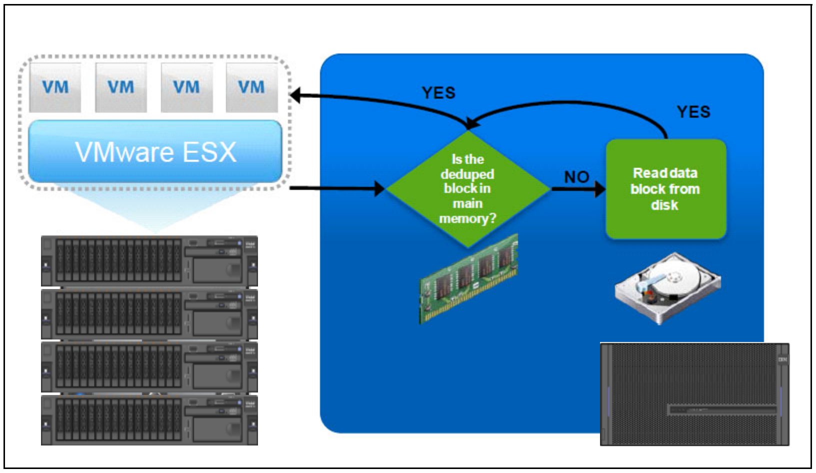

VM
VM
VM
VM
VMware ESX
YES
YES
Is the deduped block in main memory?
NO
Read data block from disk

Figure 14-5 VST with data deduplication

14.1.2 N series Virtual Storage Tiering

The N series Virtual Storage Tiering lets you scale performance and capacity and achieve the highest level of storage efficiency.

N series Virtual Storage Tier (VST) is a self-managing, data-driven service layer for storage infrastructure. It provides real-time assessment of workload-based priorities and optimizes I/O data requests for cost and performance—without requiring complex data classification. Default data placement is to the lowest-cost physical storage available (usually high-capacity SATA), because VST uses intelligent caching to leverage flash-based technology with minimal I/O and CPU overhead. On-demand data promotion is based on actual usage patterns, ensuring immediate response to changing workload demands.

As IBM's automated storage tiering (AST) approach, VST is fully compatible with both SAN and NAS environments and related data protection and business continuity requirements.

Built on the IBM fundamental strengths in storage efficiency and intelligent caching, Virtual Storage Tier provides:

- Real-time, data-driven response to your most demanding application workloads.
- Full flash technology integration: both PCIe and solid-state disk (SSD).
- Industry-leading efficiency through data deduplication and thin cloning integration.
- Out-of-the-box operation: Set it and forget it.

Virtual Storage Tier Advantages

The N series Virtual Storage Tier provides fully automated use and optimization of Flash technology, both controller-based PCI-e-based Flash and solid-state disk (SSD).

IBM N series Flash Cache PCI-e modules improve performance for workloads that are random read intensive, reducing latency by a factor of 10 or more compared to hard disk drives.

Flash Cache modules are available in capacities up to 1 terabyte and provide controller-based caching.

IBM N series Flash Pool provides caching of both random read and write operations through automated use of SSD drives, enabling the use of capacity optimized hard disk drive technology across the majority of application workloads.

Flash Pool enables the creation of a Data ONTAP software RAID-protected aggregate that is comprised of a combination of hard disk drives (HDDs) and solid-state disk drives.

With Flash Cache and Flash Pool you can significantly decrease the cost of your disk purchases and make your storage environment more efficient. Specific workload testing showed the following.

File Services Workload: Combining Flash Cache with SATA disks can significantly improve I/O throughput and response time (compared to high-performance HDD configurations) while lowering the cost per terabyte of storage by 34% and saving 40% on power.

OLTP Workload: Combining Flash Pool with SATA disks can match the performance of high-performance HDD configurations (Fibre Channel or SAS) while providing up to 350% more capacity, lowering the cost per terabyte of storage by 68%, and saving 25% on power.

When placing a pool of VMs on a aggregate that is utilizing the Virtual Storage Tier technology, changes in the required performance on individual VMs will automatically rebalance the workload across the VMs existing in that aggregate.

Real-time data promotion

Real-time promotion of hot data with high granularity. A data block typically enters the Virtual Storage Tier the first time it is read from disk. The performance benefit occurs in real time as subsequent reads are satisfied from the Virtual Storage Tier. Patterns of read behavior are identified and blocks of data that are likely to be needed are read ahead of time, but the Virtual Storage Tier never does wholesale movement of data from one tier of storage to another. This keeps usage of HDD I/O and other system resources to a minimum. The efficiency of this approach, combined with the ability to operate at the granularity of a single 4KB block, allows real-time promotion of hot data as shown in Figure 14-6.

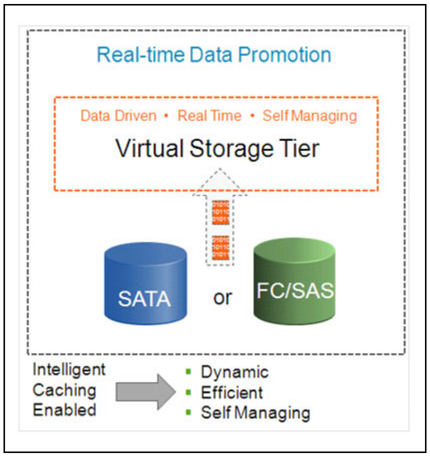


Figure 14-6 Data promotion

With migration-based AST, hot data is migrated from one storage tier to another either as a background task or scheduled during off-peak hours (to minimize the extra load on the storage system). Because these solutions typically operate at a level of granularity that is a minimum of 128 times higher than the Virtual Storage Tier (ranging from 0.5MB up to 1GB or even an entire volume or LUN), data movement can take considerable time. Such approaches might miss important spikes of activity when those spikes have a shorter duration than the time needed to identify and promote hot data.

The 4KB granularity of the Virtual Storage Tier means that it uses Flash-based media very efficiently. Solutions with coarser granularity are likely to include a lot of “cold” data along with each hot data block, and are therefore likely to require a greater amount of expensive Flash media to achieve the same results.

Easy to deploy and simple to manage. The Virtual Storage Tier works with existing data volumes and LUNs. It requires no complicated or disruptive changes to your storage environment. There is no need to set policies, thresholds, or time windows for data movement. You simply install Flash technology in your storage systems. After it is accomplished, the Virtual Storage Tier becomes active for all volumes managed by the storage controller. You can then exclude user data for lower-priority volumes from the Virtual Storage Tier if desired.

Other AST solutions require incremental policy, data classification, and structural changes to existing storage infrastructure such as the creation of dedicated storage pools and migration of data.

Fully integrated. The Virtual Storage Tier is fully integrated with the N series Unified Storage Architecture, which means that you can use it with any NAS or SAN storage protocol with no changes.

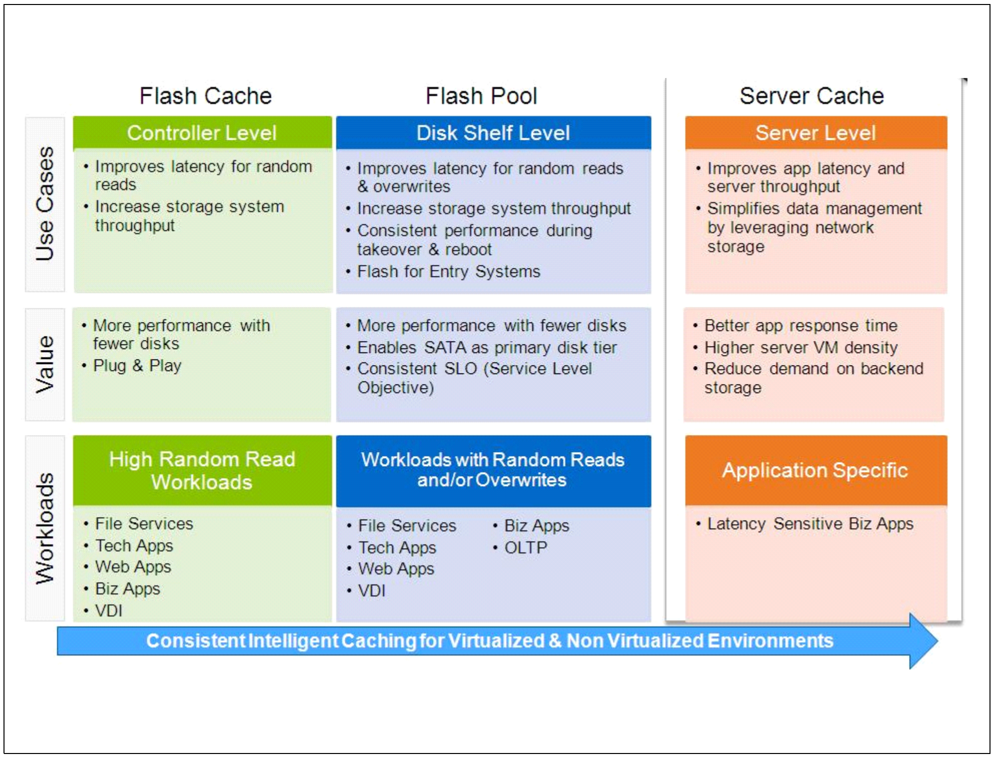
In addition, migration-based AST solutions might not interoperate with storage efficiency features such as deduplication. The N series Virtual Storage Tier works in conjunction with all N series storage efficiency features, including thin provisioning, FlexClone technology, deduplication, and compression, and this close integration works to your advantage and enhances the functioning of the Virtual Storage Tier.

For example, when you deduplicate a volume, the benefits of deduplication persist in the Virtual Storage Tier. A single block in the Virtual Storage Tier could have many metadata pointers to it, increasing the probability that it will be read again, and thus increasing the value of promoting that block. With this cache amplification a single block in the Virtual Storage Tier can serve as several logical blocks. This can yield significant performance benefits for server and desktop virtualization environments (such as shortening the duration of boot storms) while reducing the amount of Flash media needed.

14.2 Choosing VST options

Choosing the best VST level or levels is really about getting the most return for your investment in Flash by accelerating all the workloads that need to be sped up for the lowest cost (see Figure 14-7):

- Server level *(Flash Accel)*. Provides acceleration for one or more VMs running on a particular ESX host.
- Disk subsystem level *(Flash Pool)*. Provides acceleration for workloads on a per-aggregate basis.
- Controller level *(Flash Cache)*. Accelerates all workloads associated with a storage controller.



	Flash Cache	Flash Pool	Server Cache
	Controller Level	Disk Shelf Level	Server Level
Use Cases	• Improves latency for random reads • Increase storage system throughput	• Improves latency for random reads & overwrites • Increase storage system throughput • Consistent performance during takeover & reboot • Flash for Entry Systems	• Improves app latency and server throughput • Simplifies data management by leveraging network storage
Value	• More performance with fewer disks • Plug & Play	• More performance with fewer disks • Enables SATA as primary disk tier • Consistent SLO (Service Level Objective)	• Better app response time • Higher server VM density • Reduce demand on backend storage
Workloads	High Random Read Workloads • File Services • Tech Apps • Web Apps • Biz Apps • VDI	Workloads with Random Reads and/or Overwrites • File Services • Tech Apps • Web Apps • VDI • Biz Apps • OLTP	Application Specific • Latency Sensitive Biz Apps

Consistent Intelligent Caching for Virtualized & Non Virtualized Environments

Figure 14-7 Caching technology comparison

In other words, within a shared storage infrastructure you get the most workload specificity at the server level and the least at the controller level. If you need to accelerate one workload, server-level VST is a good choice. If you need to accelerate all your workloads (and possibly switch from performance-oriented to capacity-oriented disks), choose disk subsystem level or controller level.

For new deployments, we suggest starting with either Flash Cache or Flash Pool technology and then adding Flash Accel if needed to provide further performance enhancement for the most latency-sensitive applications.

When it comes to choosing between Flash Cache and Flash Pool, the following bullets summarize the similarities and differences.

- Both Flash Pool and Flash Cache provide caching for random reads and both are fully deduplication aware for maximum space efficiency.
- Flash Pool is installed and supports workloads on a per-aggregate basis. Flash Cache applies to all workloads on a controller.
- Flash Cache is plug and play, whereas Flash Pool requires some simple configuration and is then self-managed.
- Flash Pool has these capabilities:
  - Off-loads I/Os to SSD for repetitive random writes
  - Is RAID protected
  - Provides consistent performance after takeover events
  - Supports the entire N series portfolio, including the N32x0 series

In general, Flash Pool is a good choice for mission-critical applications because the benefit persists after takeover events. It's also preferred for applications that have high overwrite rates and is the only option available on the N series. Because of its proximity to main memory, Flash Cache can offer advantages for high-performance file services.

While you can install both Flash Pool and Flash Cache on the same storage system, in general there is not a big advantage to doing so. Data blocks from an aggregate that has Flash Pool enabled are never cached in Flash Cache.

With the introduction of Flash Pool and Flash Accel to VST, IBM gives you two new methods to optimize I/O performance using Flash. Remember these general guidelines:

- Flash Cache makes everything faster.
- Flash Pool makes an aggregate faster.
- Flash Accel makes an application faster.

You can combine levels to optimize overall performance while minimizing your investment. Whichever options you choose, after VST is installed, there is virtually nothing to manage. You can fine-tune your deployment if needed, but the defaults work well in most cases and the benefits are significant and measurable.

14.2.1 Flash Pool

A N series Flash Pool works at the level of the N series aggregate. (An aggregate is a collection of RAID groups.) A Flash Pool is created simply by adding a RAID group composed of solid-state disks (SSDs) to an existing 64-bit aggregate, creating a hybrid disk array that gets the best from both technologies. The SSDs are used to store random reads and repetitive random writes (overwrites) for the volumes within the aggregate, off-loading this work from hard disk drives (HDDs). As a result you can achieve the same level of performance (with better overall latency) using fewer disk spindles or using capacity-oriented disks rather than performance-oriented disks. Flash Pool gives you the latency and throughput advantages of SSD and the mass storage capacity of HDD.

The disk subsystem–level Flash Pool approach offers a number of advantages:

- Persistence. Because it is implemented in the disk layer, Flash Pools persist and remain operational when a takeover event occurs. In an HA configuration, if one controller goes offline for a planned or unplanned outage, the other controller takes over its aggregates and volumes, including Flash Pools. RAID provides resiliency to protect the data within the Flash Pool.
- Random read and random overwrite caching. From the perspective of an HDD, the most “expensive” activities are random reads and random overwrites of existing blocks. Flash Pool technology off-loads these operations to SSDs. Caching overwrites populates the Flash Pool with blocks that are likely to be reread, and prevents short-lived writes from being written to HDD.
- Deduplication awareness. Flash Pool technology is fully deduplication aware. A deduplicated block can have many references, such as when many nearly identical virtual machine instances are deduplicated. Although a deduplicated block is accessed through multiple references, only one instance of that block is kept in SSD. Less Flash is needed to accommodate a given workload as a result of this efficiency. This effect is sometimes referred to as cache amplification.
- Support for N series N32x0. Because of their compact size, N series N32x0 series controllers do not support controller-level VST, but they can utilize Flash Pool technology.

How Flash Pool works

To understand how Flash Pool technology works, you need to understand the processes for identifying and delivering random reads and random overwrites to SSD. The first time a block is read it is read into storage controller memory from disk, and the read event is categorized as random or sequential. As blocks that are categorized as random age out of controller memory they are written to SSD. Subsequent reads of the same block are then satisfied from SSD.

For writes, Data ONTAP is write optimized by design. It uses an efficient NVRAM to journal incoming write requests so that they can be acknowledged to the writer without delay. Writes are collected and written to disk in full stripes whenever possible, driving optimal performance from the underlying RAID implementation and HDDs by turning a collection of writes into sequential write activity.

The goal with Flash Pool is to off-load I/Os from HDD while enabling blocks that are likely to be reread or rewritten to end up on SSDs. Large sequential writes are handled efficiently by HDDs. Keeping them on SSDs would be a suboptimal use of resources. Random writes, and particularly blocks that are being repeatedly overwritten, turn out to be the ideal candidates to target to Flash Pool SSDs. Flash Pool populates SSDs with blocks that are likely to be read and blocks that are written repeatedly.

When a write request is received, Data ONTAP verifies that the write is random rather than sequential and that the previous write to the same block location was also random. If so, that write goes to SSD.

How blocks are evicted from a Flash Pool

Data ONTAP technology maintains a heat map (stored on SSD for persistence) that keeps track of how “hot” each block is. Reads enter the Flash Pool at “neutral.” A subsequent read elevates the temperature of the block to “warm” and then to “hot.” Writes also enter the Flash Pool at “neutral.” Subsequent overwrites do not elevate the temperature of the block, however.

When available SSD space runs low, Data ONTAP begins running an eviction scanner that decrements the temperature of each block on each pass. For example, “hot” blocks become “warm,” “warm” blocks become “neutral,” and “neutral” blocks become “cold.” If a block is read or overwritten between scanner passes, its temperature is again incremented; “hot” remains the maximum for reads and “neutral” is the maximum for overwrites. If a “cold” block is not read or overwritten, it is decremented to a temperature of “evict” on the next scanner pass. At this point, “read” blocks are evicted while overwrite blocks are scheduled to be written to HDD.

This mechanism enables only hot data to remain in a Flash Pool when it becomes full. Flash Pool adjusts dynamically to retain hot data, and the amount of a Flash Pool dedicated to reads versus overwrites depends solely on the particulars of the workloads using the pool.

Figure 14-8 shows how blocks are evicted from a Flash Pool based on a heat map. When the pool is full, an eviction scanner decrements the “temperature” of each block on each pass. Blocks are evicted when they reach a temperature of “evict.” Accesses between scanner passes increment the temperature of a block, so “hot” data remains in the Flash Pool.

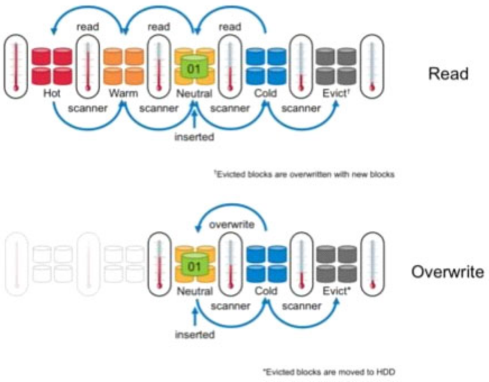
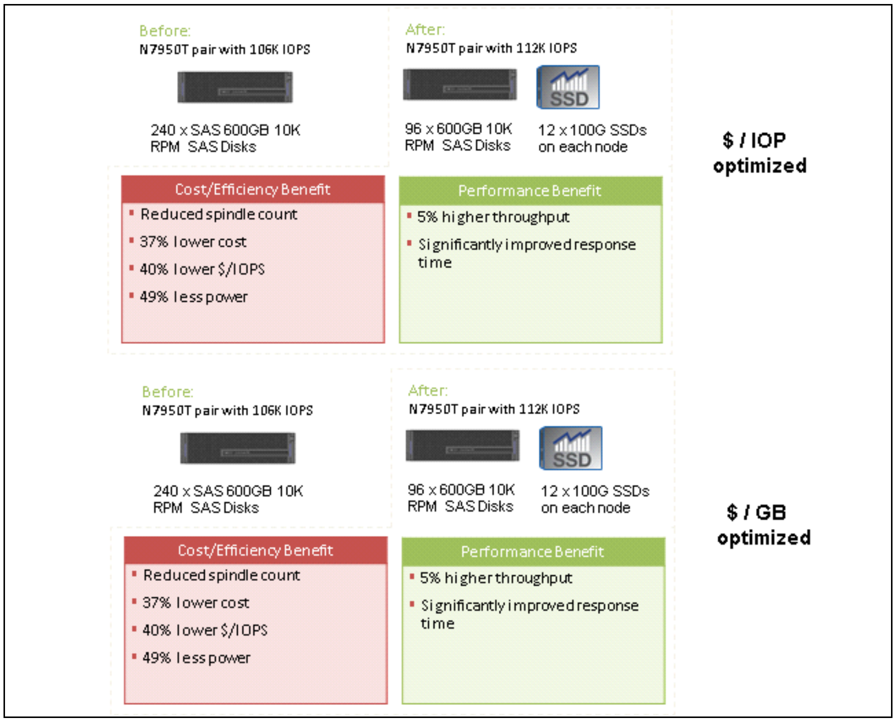


Figure 14-8 How Flash Pool works

Flash Pool performance

Although we have not published any benchmarks yet using Flash Pool technology, IBM has undertaken some comparative before-and-after studies using an OLTP workload to illustrate the potential impact. Starting from the same N7950T base configuration, we implemented Flash Pool, optimized in one case for cost per IOPS and in the second for cost per GB of storage. Results are shown in Figure 3. Note that both cases result in a significant improvement in overall latency, which can have a bigger impact on perceived performance than total IOPS in many cases.

Impact of Flash Pool on cost/efficiency and performance is shown in Figure 14-9.



Before:
N7950T pair with 106K IOPS

240 x SAS 600GB 10K RPM SAS Disks

After:
N7950T pair with 112K IOPS

96 x 600GB 10K RPM SAS Disks

12 x 100G SSDs on each node

Cost/Efficiency Benefit
- Reduced spindle count
- 37% lower cost
- 40% lower $/IOPS
- 49% less power

Performance Benefit
- 5% higher throughput
- Significantly improved response time

$ / IOP optimized

Before:
N7950T pair with 106K IOPS

240 x SAS 600GB 10K RPM SAS Disks

After:
N7950T pair with 112K IOPS

96 x 600GB 10K RPM SAS Disks

12 x 100G SSDs on each node

Cost/Efficiency Benefit
- Reduced spindle count
- 37% lower cost
- 40% lower $/IOPS
- 49% less power

Performance Benefit
- 5% higher throughput
- Significantly improved response time

$ / GB optimized

Figure 14-9 Flash Pool cost/efficiency x performance

Table 14-1 shows Flash Pool requirements and options.

Table 14-1 Flash Pool requirements

Flash pool requirements and options	
Data ONTAP version	Data ONTAP 8.1.1 or later, 7-Mode and Cluster-Mode
Tuning options (per volume)	
Read	Random-read (default) Meta: Metadata only Random-read-write: Populates read pool with random reads AND writes None: Disables read caching for a volume
Write	Random-write (default) None: Disables write caching for volume
Supported Platforms	N32x0, N62x0, N7950T, and V-Series using N series disk and SSD only

14.2.2 Flash Cache

Flash Cache is a PCI Express card that can be installed many of the current N series storage controller systems (Figure 14-10). Each module contains either 256 GB, 512 GB, or 1 TB of SLC NAND Flash. In the VMware solution on N series, we recommend having at least one Flash Cache device per N series storage cluster.

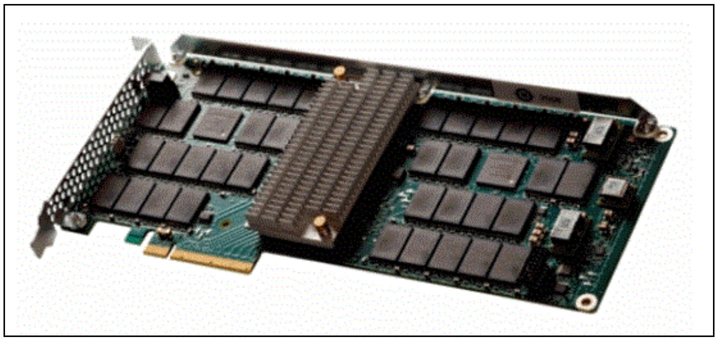


Figure 14-10 Flash Cache card

How Data ONTAP VST functions with Flash Cache

VST can be extended with the use of Flash Cache. As long as that block has not been evicted from both caches, all subsequent reads are performed from main memory or Flash Cache, thus improving performance by not having to go to disk. Again, the more heavily the data is deduplicated and the more frequently accessed, the longer it stays in cache. Transparent storage array caching combined with N series disk deduplication provides cost savings on many levels. Figure 14-11 shows transparent storage array caching with Flash Cache and deduplication.

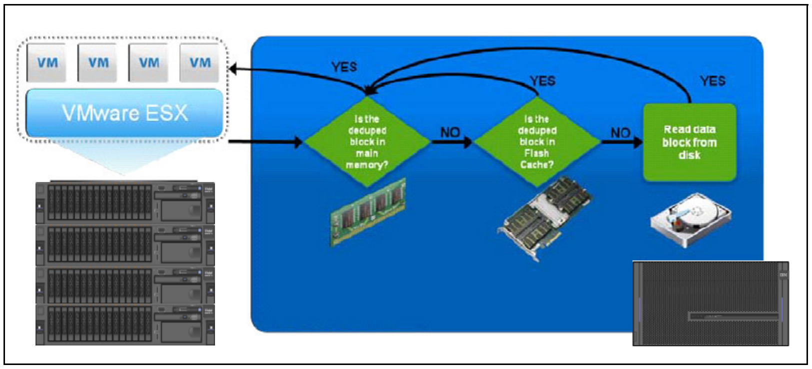

VM
VM
VM
VM
VMware ESX
YES
YES
YES
Is the deduped block in main memory?
NO
Is the deduped block in Flash Cache?
NO
Read data block from disk

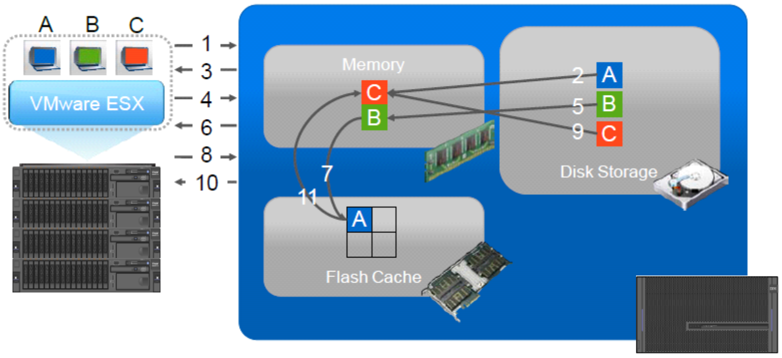
Figure 14-11 Transparent storage array caching with Flash Cache and deduplication

The decision whether to use Flash Cache in addition to Data ONTAP VST is based on the amount of deduplicated data and the percentage of reads within the environment. As users of the VMware View environment create more data, the amount of deduplicated data changes, thus affecting the cache hit rate. Thus, more cache might be needed if the data becomes more unique (even after running regular deduplication operations on the new data).

We recommend when possible to use Data ONTAP 7.3.1 (Data ONTAP 7.3.2 when using Flash Cache) or later for VMware environments. For environments with greater than 500 virtual machines per N series storage controller, we recommend the use of both Data ONTAP caching and at least one Flash Cache device per storage controller.

How Flash Cache functions without deduplication (traditional caching)

Flash Cache works by receiving data blocks that have been evicted from main memory. After being evicted from main memory, if the same block should be requested a second time and that block has not been evicted from Flash Cache, that block is read from Flash Cache and placed into main memory. Every block, whether or not it contains the same data as another block, is read first from disk. It is how legacy storage arrays operate in that the first of all reads must come from disk, and subsequent reads depend on the size of the cache. It is the reason legacy vendors require large amounts of cache. Figure 14-12 shows Flash Cache without deduplication.



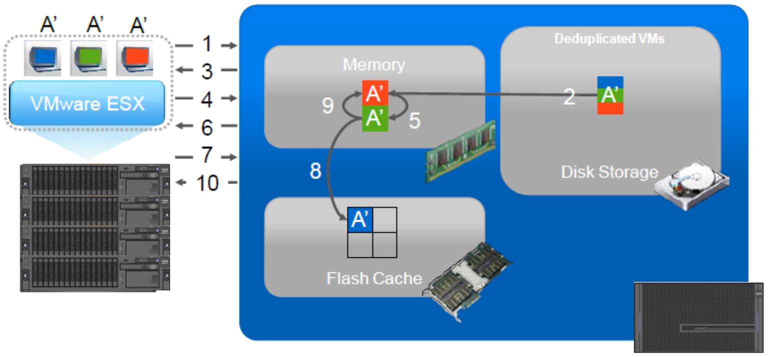
1. Block A (blue) requested from client.
2. Block A (blue) read from disk to memory.
3. Block A (blue) returned to client.
4. Block B (green) requested from client.
5. Block B (green) read from disk to memory.
6. Block B (green) returned to client.
7. Block A (blue) evicted from memory to Flash Cache because memory is full.
8. Block C (orange) requested from client.
9. Block C (orange) read from disk to memory.
10. Block C (orange) returned to client.
11. Subsequent reads of block A (blue) or B (green) result in the eviction of blocks C (orange) and reads from Flash Cache.

Figure 14-12 Flash Cache without deduplication

How Flash Cache functions with deduplication (transparent storage array caching)

Flash Cache receives data blocks that have been evicted from main memory. After eviction from main memory, if a block should be required for a second time, that block is read from Flash Cache, a cache hit, and placed into main memory. If the block being requested is a duplicate block that has been deduplicated (also known as a shared block), the block is read from Flash Cache to main memory. As long as that block is not evicted from cache, all subsequent reads are performed from Flash Cache, thus improving performance by not having to go to disk. Transparent storage array cache combined with N series disk deduplication provides cost savings on many levels.

Figure 14-13 shows Flash Cache with deduplication.



1. Block A' (blue) requested from client.
2. Block A' (blue) read from disk to memory.
3. Block A' (blue) returned to client.
4. Block A' (green) requested from client.
5. Block A' (green) read from memory.
6. Block A' (green) returned to client.
7. Block A' requested from client.
8. Block A' (blue) evicted from memory to Flash Cache because memory is full and it was the first block.
9. Block A' (orange) read from memory.
10. Block A' (orange) returned to client.

Figure 14-13 Flash Cache with deduplication

FlexScale

FlexScale is the tunable software component of Flash Cache. It is a licensed feature of Data ONTAP 7.3 or greater. FlexScale allows different caching modes to be used based on the type of workload. The different modes of caching are metadata only, normal user data, and low-priority blocks. Extensive scalable VMware testing within the N series solution labs has shown that significant performance improvements can be gained by turning on metadata and normal user data caching modes in FlexScale.

To license and enable FlexScale:

1. Connect to the controller system's console, using either SSH, telnet, or serial console.
2. Check to see if the FlexScale license has already been installed by typing license and finding the line that says flex_scale:

   ```
   license
   ```

3. If FlexScale is not licensed, you can license it by issuing the following command. If you do not have your license available, you can locate it within the N series support site.

   ```
   License add <License_Key>
   ```

To change the FlexScale caching modes for use with VMware workloads:

1. Connect to the controller system’s console, using either SSH, telnet, or serial console.
2. Change the following options with the following commands, which turn on metadata and normal user data block caching. They are the recommended FlexScale settings for VMware:

   ```
   options flexscale.enable on
   options flexscale.normal_data_blocks on
   ```

3. You can verify these settings have been changed:

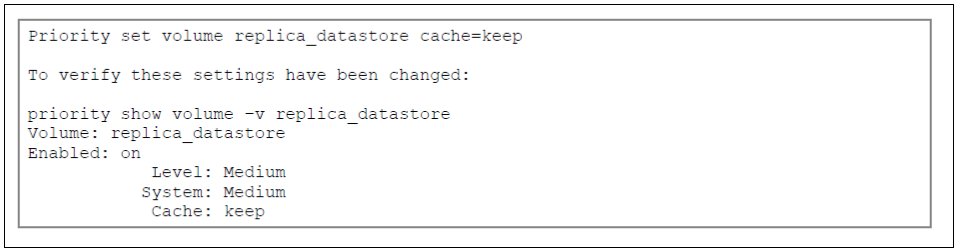
   ```
   options flexscale
   ```

FlexShare

FlexShare is a feature of Data ONTAP that allows administrators to set QoS policies on different volumes and data types. When a N series storage controller is being configured in a VMware clones environment, the FlexShare caching policy of keep should be set on the datastore used to store the replica disks.

To change the FlexShare caching modes for use with VMware clones:

1. Connect to the controller system’s console using either SSH, telnet, or serial console.
2. Change the following options with the commands noted (see Figure 14-14). This turns on the FlexShare policy to keep the data from the select volume in Flash Cache. They are the recommended FlexShare settings for VMware View linked clone replica datastores.



```
Priority set volume replica_datastore cache=keep

To verify these settings have been changed:

priority show volume -v replica_datastore
Volume: replica_datastore
Enabled: on
            Level: Medium
           System: Medium
            Cache: keep
```

Figure 14-14 Volume FlexShare policy setting

14.2.3 Flash Accel

Flash Accel is designed to extend the benefits of N series VST across the network to encompass the server itself. Having local Flash devices on a server means that you have direct-attached storage that you have to manage. It creates potential problems with data protection and isolates silos of data. Server caching with Flash Accel eliminates these problems.

Flash Accel benefits

Server caching with Flash Accel offers a number of advantages.

Dedicate Flash. Use it to enhance performance of a particular application. Flash Accel lets you pinpoint Flash use for the benefit of one or a few applications while eliminating the disadvantages of local storage, increasing throughput by up to 80%, and reducing transaction latency by up to 90%.

Hardware agnostic. Flash Accel will work with any enterprise-class Flash device(s) (PCI-e card or SSD) that you have on your server.

Persistent and durable. Data stored in the Flash Accel cache is able to persist through a server reboot. The cache even remains durable to events such as failures and blue screens.

Unique cache coherency. When an event such as a restore changes data on back-end storage, other caching solutions resort to dumping the entire server cache, resulting in a long period of reduced performance while it is repopulated. N series Flash Accel is able to identify and evict just the blocks that have changed, preserving performance.

Increases VM density. Because VMs and applications run more smoothly and spend less time blocked waiting for resources, you can actually increase the number of VMs per server—5 to 10 additional VMs is typical.

Improves efficiency of back-end storage. Tests show that Flash Accel improves the efficiency of back-end storage by 40% versus the same configuration and workload without Flash Accel enabled. This reduces the resources required on back-end storage and frees up resources to support other workloads.

Low overhead. Flash Accel requires only about 0.5% of the memory resources of the ESXi host.

Data protection. Data stored in a server-side cache is also stored on N series storage, where it can be protected using standard N series methods.

The first release of Flash Accel works with VMware vSphere 5.0 or higher and Windows VMs only. Future releases will expand support to include additional VMs, other hypervisors, and bare metal.

How Flash Accel works

Flash Accel consists of three components:

N series vCenter VSC plug-in. Configuration and management of Flash Accel is accomplished using a plug-in for the N series Virtual Storage Console (VSC), which runs in VMware vCenter. This plug-in allows you to perform these tasks:

- Install and configure the ESXi hypervisor plug-in driver.
- Install and configure guest Flash Accel agents.
- Discover Flash SSD devices on ESXi hosts.
- Configure one or more SSD or other Flash devices on ESXi hosts for use by Flash Accel.
- Enable/disable caching on host.
- Resize the cache on a guest VM.
- Report on current cache state and performance metrics.

Flash Accel hypervisor plug-in (installed on the ESXi host). The hypervisor plug-in is installed on an ESXi host and establishes control over locally attached devices (such as SSDs) and storage array paths according to the configuration you define using VSC. The plug-in creates logical devices and presents them to the ESXi storage stack as SCSI devices. Logical devices created on multiple ESXi hosts with the same WWN allow ESXi to treat a device as a shared device so that VMs using these devices can participate in vMotion and VMware HA operations. In addition to being able to migrate the VMs, the hypervisor plug-in provides management of the Flash device and can enable dynamic resource sharing and cache block deduplication.

Flash Accel agent in Windows VM. A user-level agent is implemented for Windows guest VMs. This agent has the following functions:

- Passes configuration to the filter driver
- Enables/disables caching of one or more devices or an entire VM
- Communicates performance metrics to VSC
- Integrates with other data management software like SnapDrive and SnapManager technologies

The service agent exports a Web service to VSC and communicates with the drive by Windows PowerShell cmdlets.

As shown in Figure 14-15, Flash Accel includes agents that run in each VM and a plug-in for VMware vSphere, and it is controlled from N series VSC running within vCenter. It can use any PCI-e Flash card or SSD available on an ESXi host.

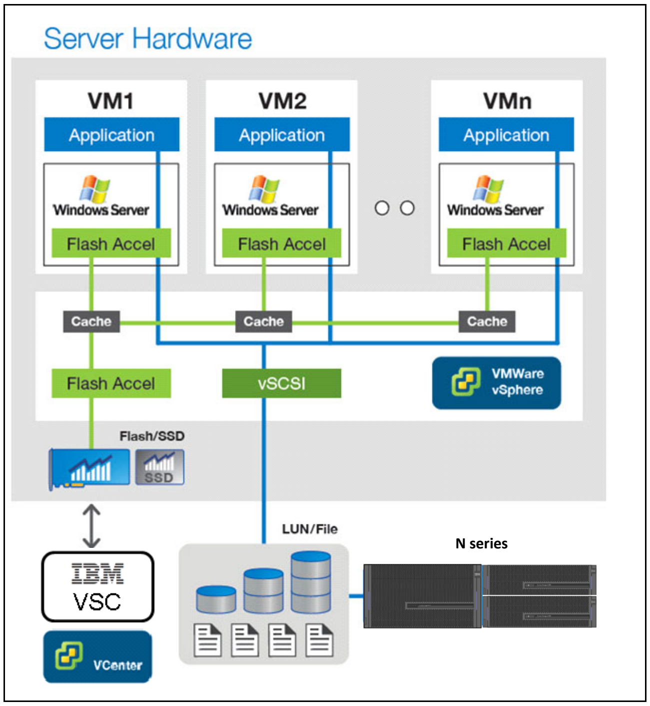


Figure 14-15 Flash Accel on VMware environment

All reads from the VM are cached locally for reuse, off-loading future reads from back-end storage. Writes are written through to back-end storage but available for rereading from cache.

The Flash Accel cache has two key areas, cache operations and storage manager:

- The **cache operations** layer is responsible for implementing the interfaces for sending I/O requests through the cache; it includes translating incoming I/O requests into a number of 4KB I/O requests to or from the cache and/or the primary storage server. The cache operations layer is entirely implemented in the Windows filter driver.
- The **storage manager** is responsible for the layout of the metadata and cached data blocks on Flash and the implementation of persistence. This module is called only by the cache operations layer. The storage manager resides within the filter driver and the hypervisor initializes, configures, and manages the Flash device.

Data coherency is the most important feature of Flash Accel. If back-end data is changed without notifying Flash Accel, it is possible to have the cache data and the back-end storage data out of sync. It would result in incorrect data being returned to the application/end user from the cache, which would cause data corruption. There are two situations in which data coherency is an issue:

- Online data modification where data is modified in band. Flash Accel checks for incoherency when there is a device mount/unmount/boot by comparing cached metadata with that from the storage system to spot incoherency and invalidate blocks as appropriate. An example of this would be a SnapRestore operation of application data on N series storage. In between the checks, there is no incoherency issue because Data ONTAP will not modify data when a VM is actively using it. Out-of-band modification (in which the administrator updates a running VM by some means the storage is not aware of) is not supported.
- Offline data modification (for example, VMDK/LUN restore). Flash Accel takes the same action of comparing cached metadata with data on back-end storage and invalidating blocks as needed. An example is using SnapRestore to restore an entire VM.

The advantage of Flash Accel in these types of situations is that it only invalidates blocks that are different while retaining all blocks that have not changed. When situations like this arise, other available solutions completely drop all cached data and rewarm the entire cache. It might take a few hours to days depending on the data, during which time performance is degraded.

15

Virtual Storage Console 4.1

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, as explained in this chapter. It includes the following topics:

- Virtual Storage Console
- Installing the Virtual Storage Console 4.1
- Adding storage controllers to the VSC
- Optimal storage settings for ESXi host
- SnapMirror integration
- VSC in an N series MetroCluster environment
- Backup and recovery
- Provisioning and cloning
- Optimum VM availability
- Scripting

© Copyright IBM Corp. 2013. All rights reserved.

15.1 Virtual Storage Console

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. They 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.

15.1.1 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 15-1, 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.

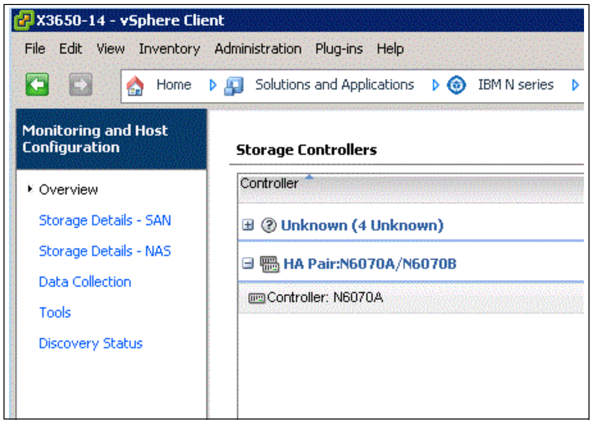


Figure 15-1 Virtual Storage Console

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.

15.1.2 License requirements

Table 15-1 summarizes the N series license requirements to perform different VSC functions.

Table 15-1 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

15.1.3 Architecture overview

Figure 15-2 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.

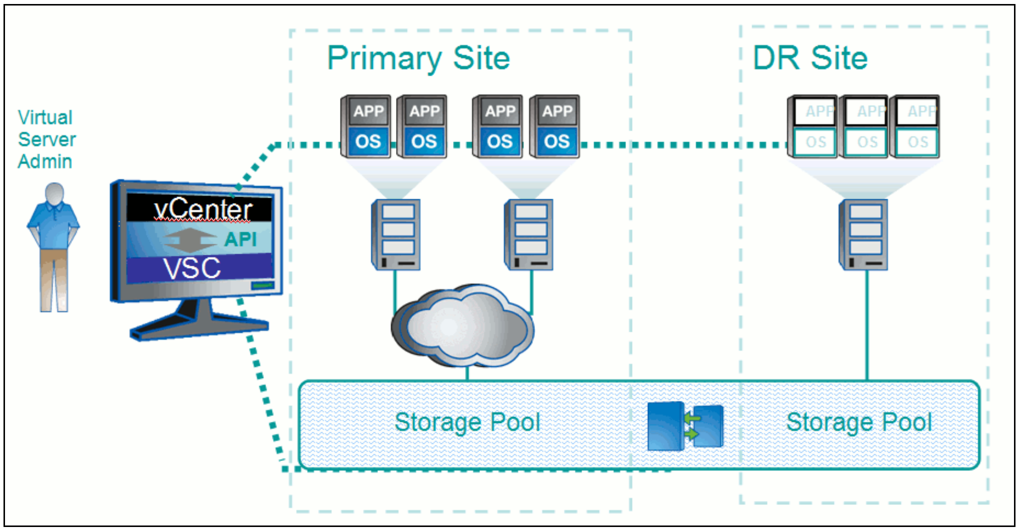


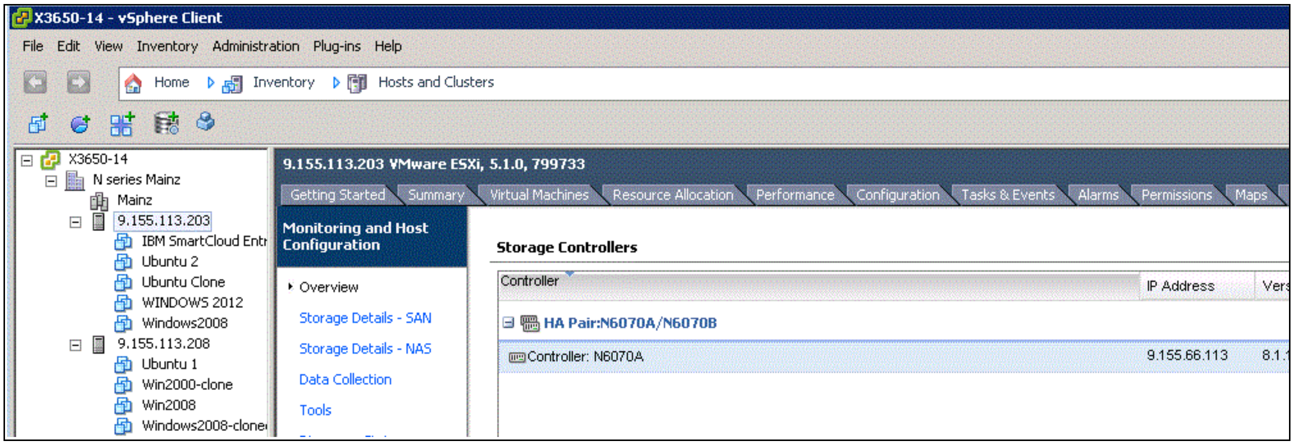
Figure 15-2 Architecture overview

15.1.4 Monitoring and host configuration

The Monitoring and Host Configuration capability enables you to manage 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 vCenter GUI to create LUNs and manage storage controllers
- Collect diagnostic information from the ESXi 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 tab in the vCenter Server and click Monitoring and Host Configuration in the navigation pane, the Overview panel displays. It is similar to Figure 15-3.



Controller	IP Address	Vers
HA Pair:N6070A/N6070B		
Controller: N6070A	9.155.66.113	8.1.1

Figure 15-3 VSC overview

Alternatively, you can find the VSC plug-in under Solutions and Applications (Figure 15-4).

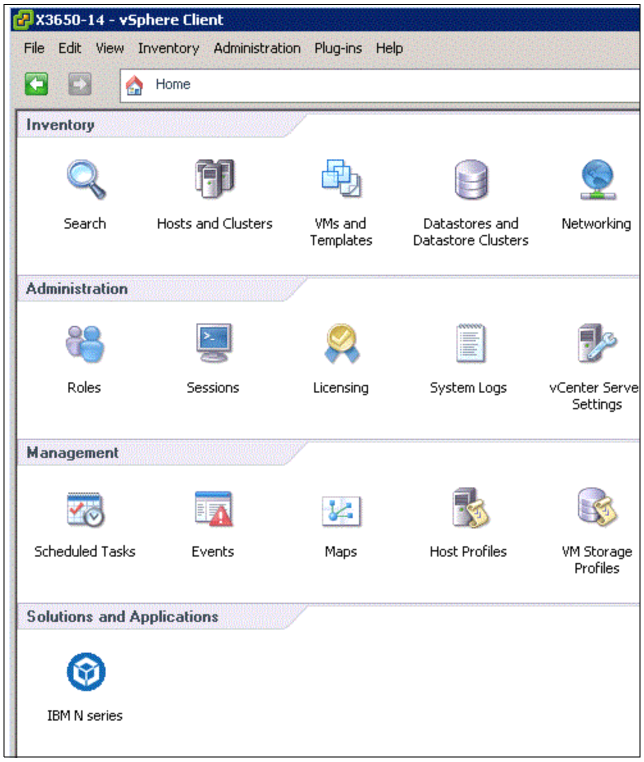


Figure 15-4 VSC location

15.1.5 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.

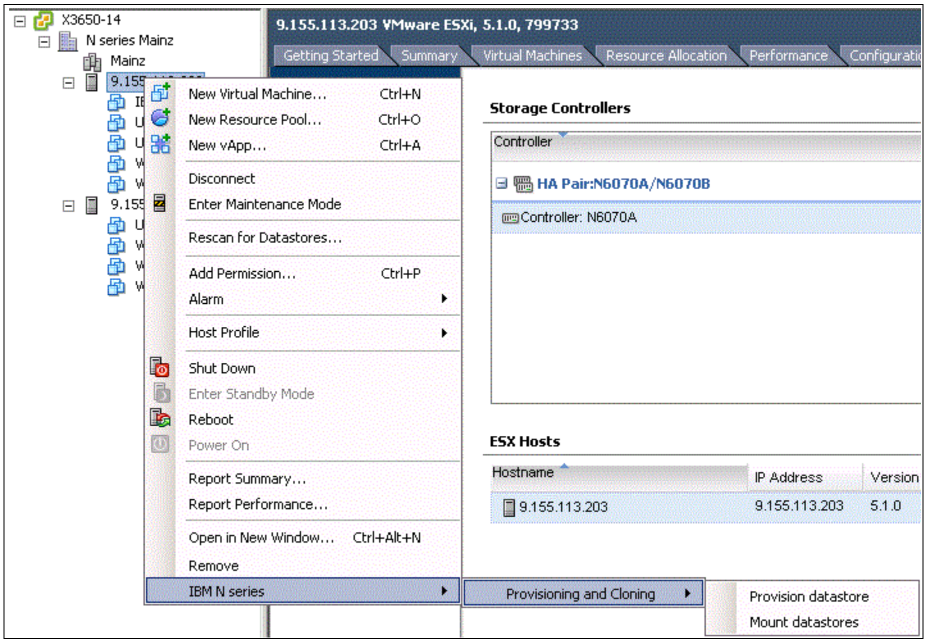
You can use the provisioning and cloning capability for the following purposes:

- 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 **IBM N series** → **Provisioning and Cloning** (Figure 15-5):

- Right-click a powered-down virtual machine or template to create clones.
- Right-click a datacenter, cluster, or host to provision datastores.



Hostname	IP Address	Version
9.155.113.203	9.155.113.203	5.1.0

Figure 15-5 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** → **IBM N series** → **Provisioning and Cloning**. 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.

15.2 Installing the Virtual Storage Console 4.1

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.

15.2.1 Basic installation

Before downloading and installing the VSC, make sure that your deployment has the required components:

- You need a vCenter Server version 5.0 or later. The VSC can be installed on the vCenter Server or on another server or VM (see Figure 15-6).
- If installing on another server or VM, this system must run 32-bit or 64-bit Windows Server 2008, 2003 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.

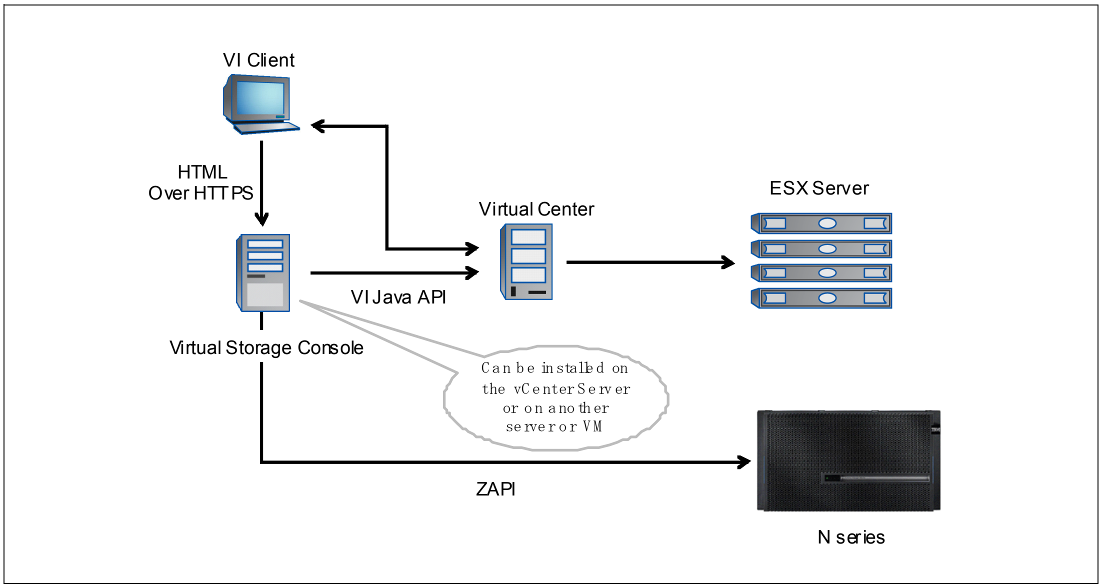


Figure 15-6 VSC possible deployments

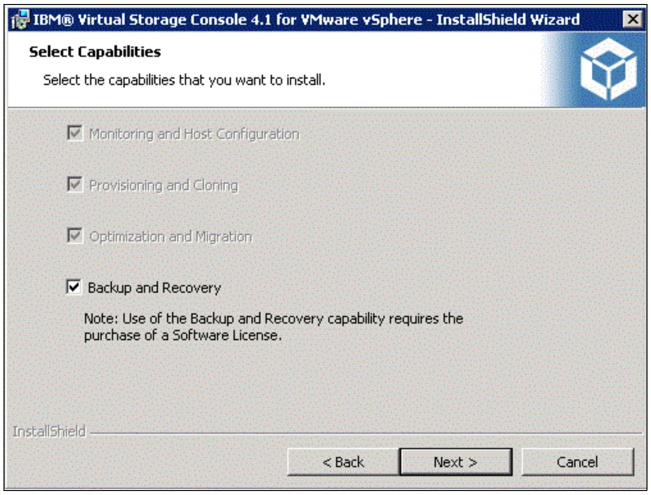
Tip: To keep it simple, we suggest installing the VSC on the vCenter server.

Complete the following steps to install the VSC 4.1:

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 15-7.

3. Follow the on-screen instructions.

   During the installation process, a prompt displays to select the features of the VSC 4.1 () 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. See Figure 15-7.



IBM® Virtual Storage Console 4.1 for VMware vSphere - InstallShield Wizard

Select Capabilities

Select the capabilities that you want to install.

☑ Monitoring and Host Configuration

☑ Provisioning and Cloning

☑ Optimization and Migration

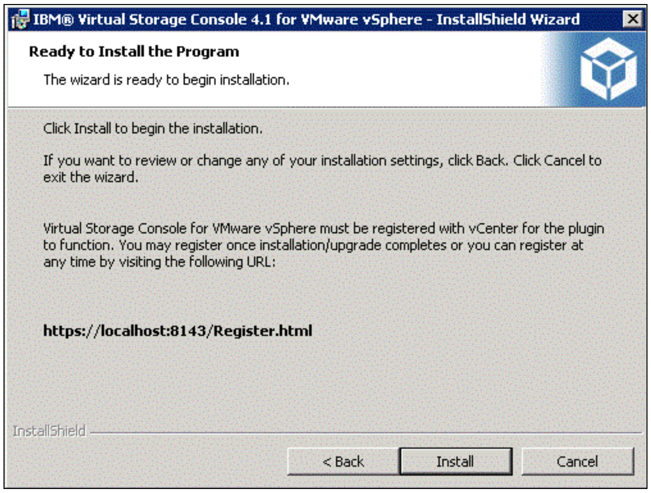
☑ Backup and Recovery

Note: Use of the Backup and Recovery capability requires the purchase of a Software License.

Figure 15-7 Select VSC features

4. Register the VSC as a plug-in, in the vCenter Server in the window that opens when the process is complete.

The installation process launches the vCenter registration process as shown in Figure 15-8.



IBM® Virtual Storage Console 4.1 for VMware vSphere - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

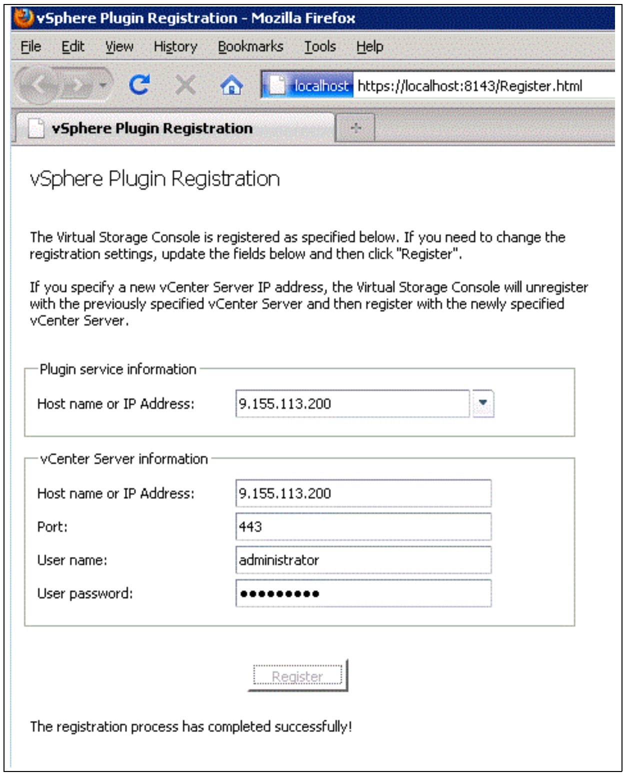
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Virtual Storage Console for VMware vSphere must be registered with vCenter for the plugin to function. You may register once installation/upgrade completes or you can register at any time by visiting the following URL:

https://localhost:8143/Register.html

Figure 15-8 vCenter registration process

5. Finally, register the VSC plug-in with a vCenter server (Figure 15-9). This final step requires a user with vCenter administrator credentials to complete the registration process.


vSphere Plugin Registration - Mozilla Firefox
File Edit View History Bookmarks Tools Help
localhost https://localhost:8143/Register.html
vSphere Plugin Registration
Register

vSphere Plugin Registration

The Virtual Storage Console is registered as specified below. If you need to change the registration settings, update the fields below and then click "Register".

If you specify a new vCenter Server IP address, the Virtual Storage Console will unregister with the previously specified vCenter Server and then register with the newly specified vCenter Server.

Plugin service information

Host name or IP Address: 9.155.113.200

vCenter Server information

Host name or IP Address: 9.155.113.200

Port: 443

User name: administrator

User password: ●●●●●●●●●

The registration process has completed successfully!

Figure 15-9 VSC registration with vCenter server

15.2.2 Registration completion

Upon successful registration, the system confirms by issuing the following message on the web page: `The registration process has completed successfully!`

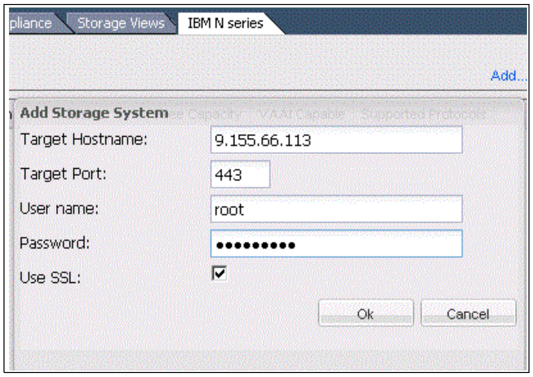
15.3 Adding storage controllers to the VSC

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 IBM N series tab 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 ESXi host in the environment. As an alternative to running discovery for the entire environment, you can select an ESXi host or cluster in the vSphere client and then select the IBM N series 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 windows pops-up, as displayed in Figure 15-10, 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.



Add Storage System

Target Hostname: 9.155.66.113

Target Port: 443

User name: root

Password: •••••••••

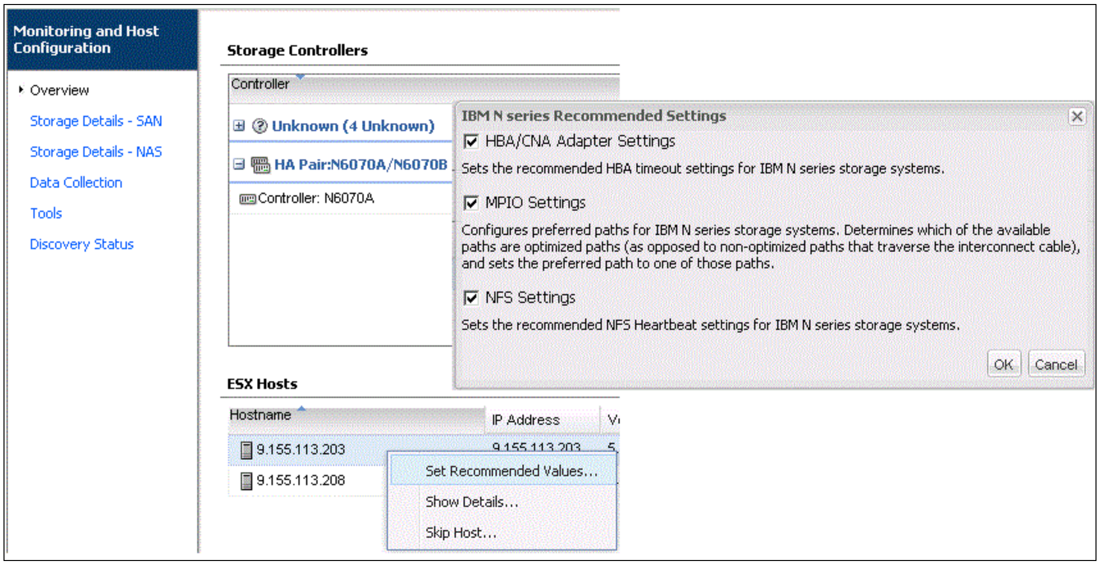
Use SSL: ☑

Figure 15-10 Adding storage controller access in VSC

15.4 Optimal storage settings for ESXi host

The VSC enables the automated configuration of storage-related settings for all ESXi 5.x hosts connected to N series storage controllers. VMware administrators can right-click individual or multiple ESXi host 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 ESXi server, and run the settings as shown in Figure 15-11.



IBM N series Recommended Settings

☑ HBA/CNA Adapter Settings

Sets the recommended HBA timeout settings for IBM N series storage systems.

☑ MPIO Settings

Configures preferred paths for IBM N series storage systems. Determines which of the available paths are optimized paths (as opposed to non-optimized paths that traverse the interconnect cable), and sets the preferred path to one of those paths.

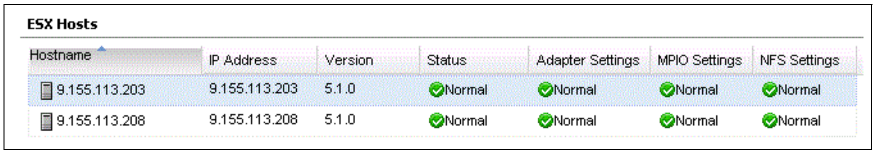
☑ NFS Settings

Sets the recommended NFS Heartbeat settings for IBM N series storage systems.

Hostname	IP Address
9.155.113.203	9.155.113.203
9.155.113.208	

Figure 15-11 Optimize ESX settings

After rebooting the ESX server, we can verify the improved settings. All status indicators are green (see Figure 15-12).



ESX Hosts

Hostname	IP Address	Version	Status	Adapter Settings	MPIO Settings	NFS Settings
9.155.113.203	9.155.113.203	5.1.0	✓Normal	✓Normal	✓Normal	✓Normal
9.155.113.208	9.155.113.208	5.1.0	✓Normal	✓Normal	✓Normal	✓Normal

Figure 15-12 Optimized ESX adapter settings

15.5 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.

15.5.1 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.

15.5.2 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.

15.6 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 15-13 provides a redundant VMware server, redundant N series heads, and redundant storage.

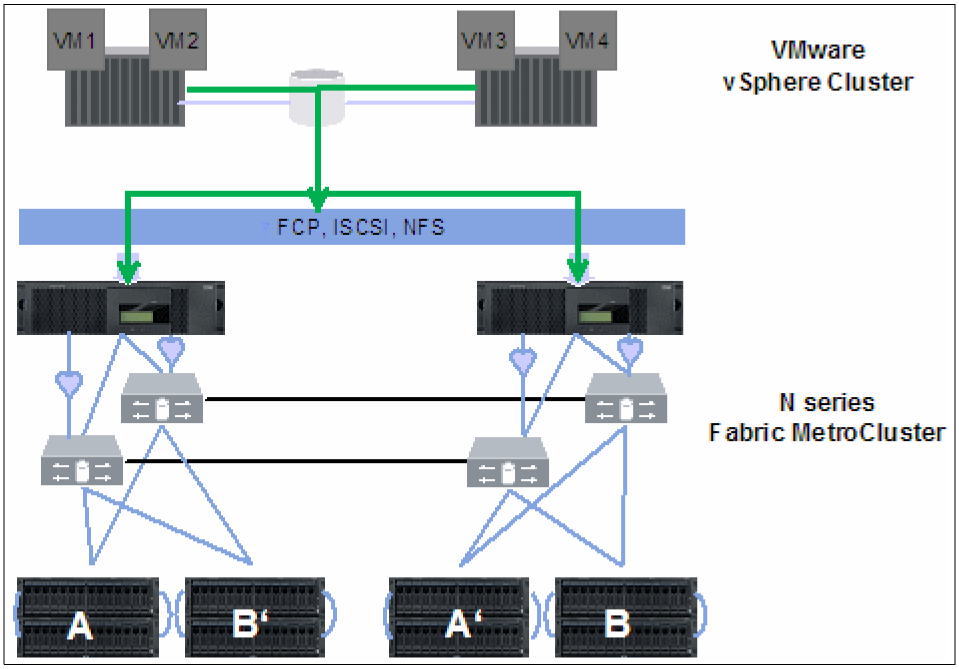


Figure 15-13 MetroCluster and VMware vSphere integrated solution

For more information about N series MetroCluster, see the “MetroCluster” chapter in the Redbooks publication, *IBM System Storage N series Software Guide*, SG24-7129.

15.7 Backup and recovery

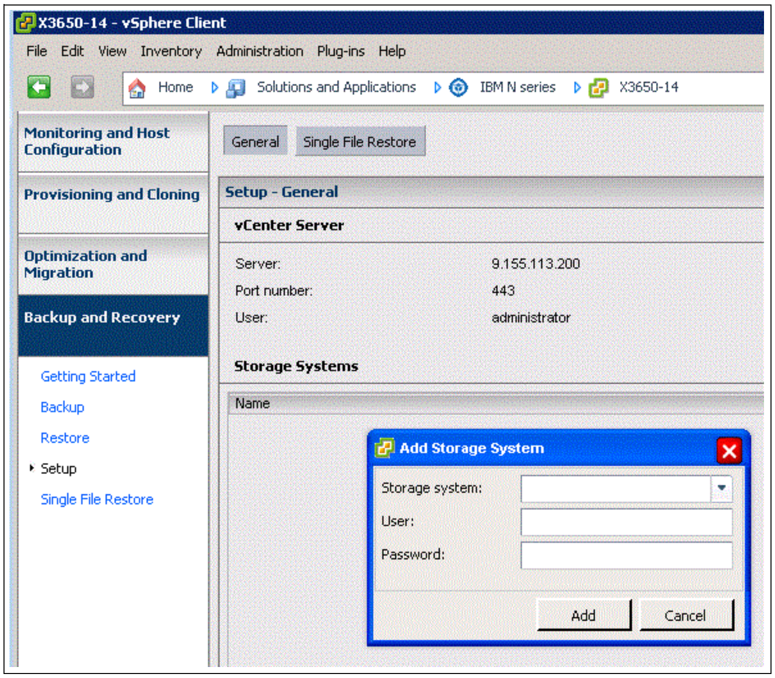
This section provides examples of backing up a single virtual machine or the entire DataCenter. The Backup and Recovery capability of the Virtual Storage Console provides rapid backup and recovery of multi-host configurations running on N series storage systems.

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 15-14.

Important: You must register your N series system two times; first, for the VSC and second, for backup and recovery.



Server: 9.155.113.200
Port number: 443
User: administrator

Figure 15-14 N series registration for backup and restore

15.7.1 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 4.1, 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 4.1, 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.

15.7.2 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.

15.7.3 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 15-15.

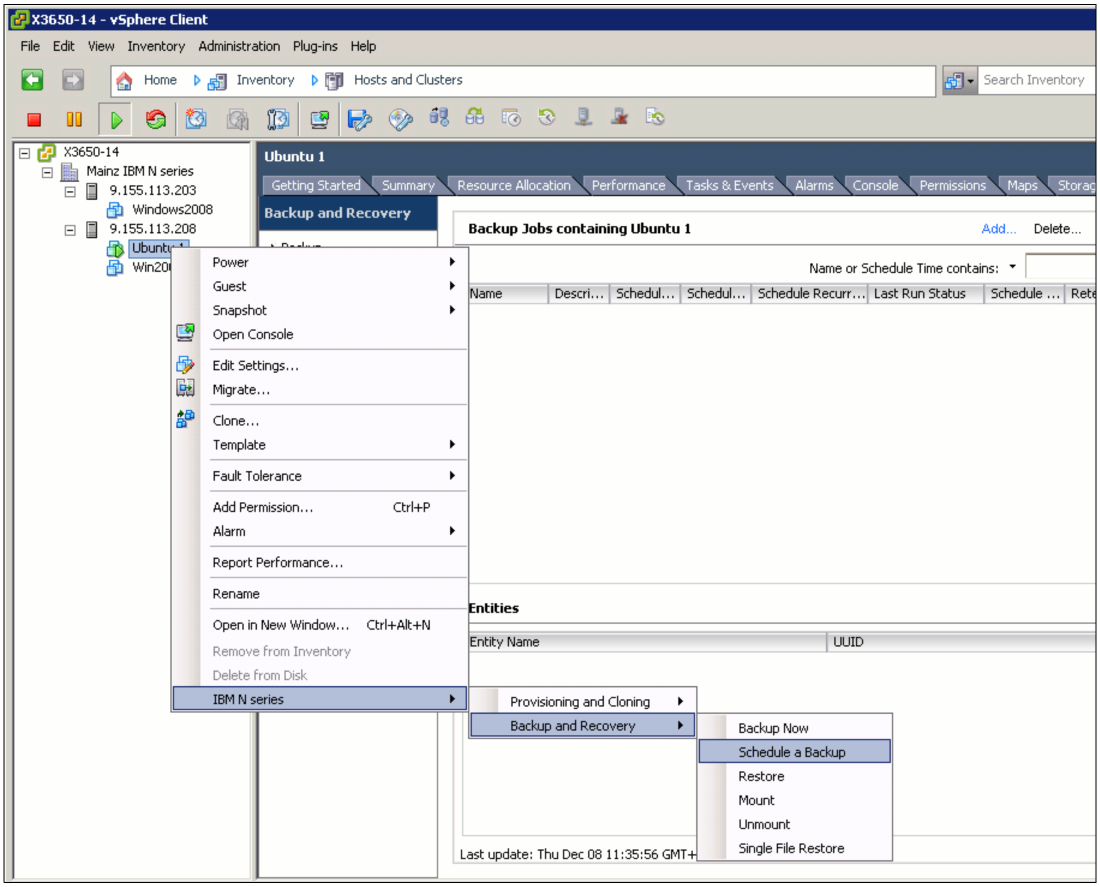
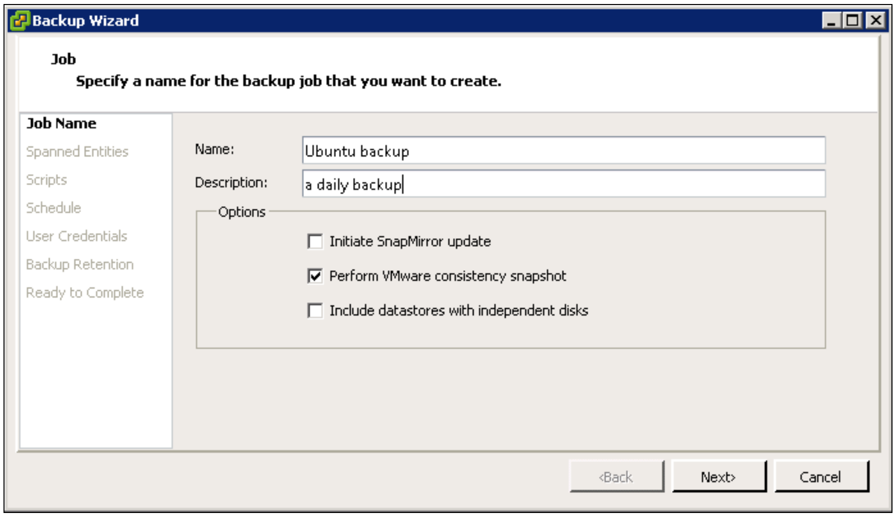


Figure 15-15 Adding a backup

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 15-16), then click **Next**.



Name: Ubuntu backup

Description: a daily backup

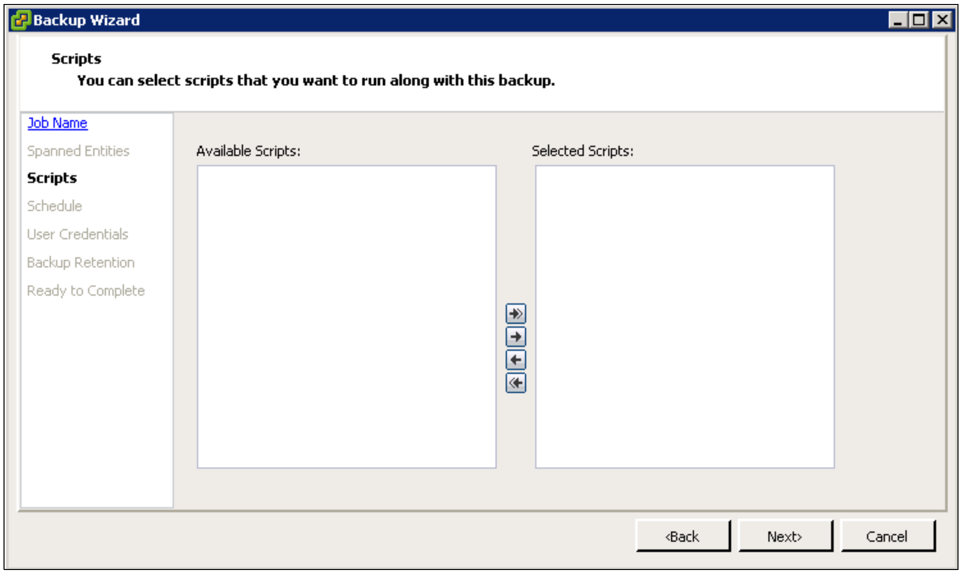
□ Initiate SnapMirror update

☑ Perform VMware consistency snapshot

□ Include datastores with independent disks

Figure 15-16 Backup options

4. In the following window, you can select scripts to be included in the backup job (see Figure 15-17).

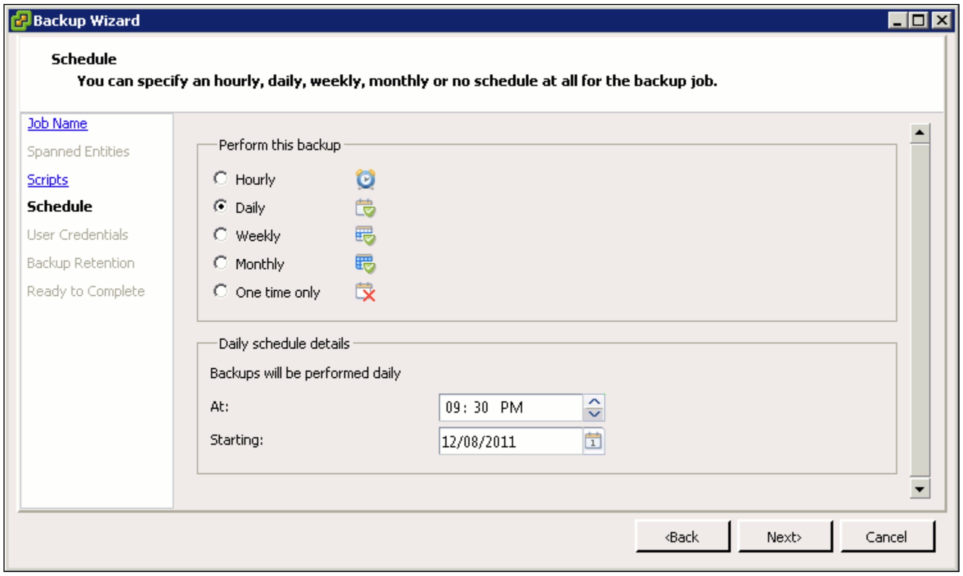


Backup Wizard

Scripts
You can select scripts that you want to run along with this backup.

Figure 15-17 Backup scripts

5. Now you can specify the schedule for the backup job as shown in Figure 15-18, and click **Next**.



Backup Wizard

Schedule
You can specify an hourly, daily, weekly, monthly or no schedule at all for the backup job.

Perform this backup

○ Hourly
● Daily
○ Weekly
○ Monthly
○ One time only

Daily schedule details

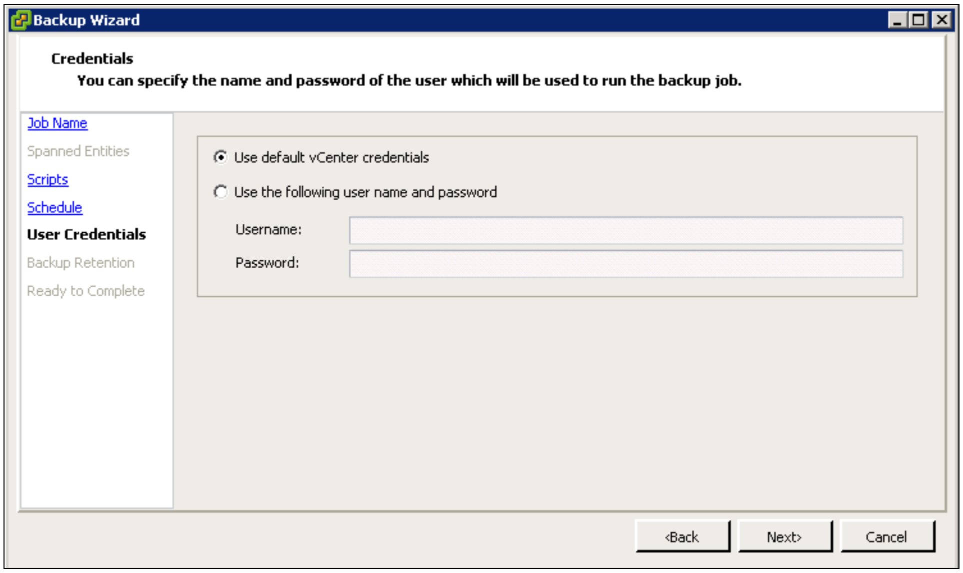
Backups will be performed daily

At: 09: 30 PM

Starting: 12/08/2011

Figure 15-18 Backup schedule

6. Confirm your credentials on the next panel as shown in Figure 15-19, and click **Next**.



Credentials

You can specify the name and password of the user which will be used to run the backup job.

● Use default vCenter credentials

○ Use the following user name and password

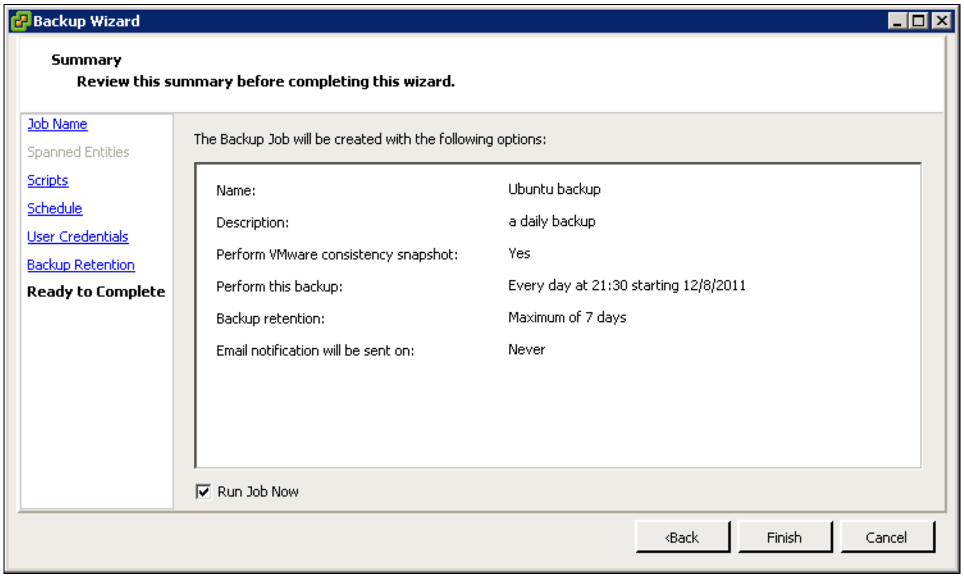
Username:

Password:

Figure 15-19 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 15-20.



Summary

Review this summary before completing this wizard.

The Backup Job will be created with the following options:

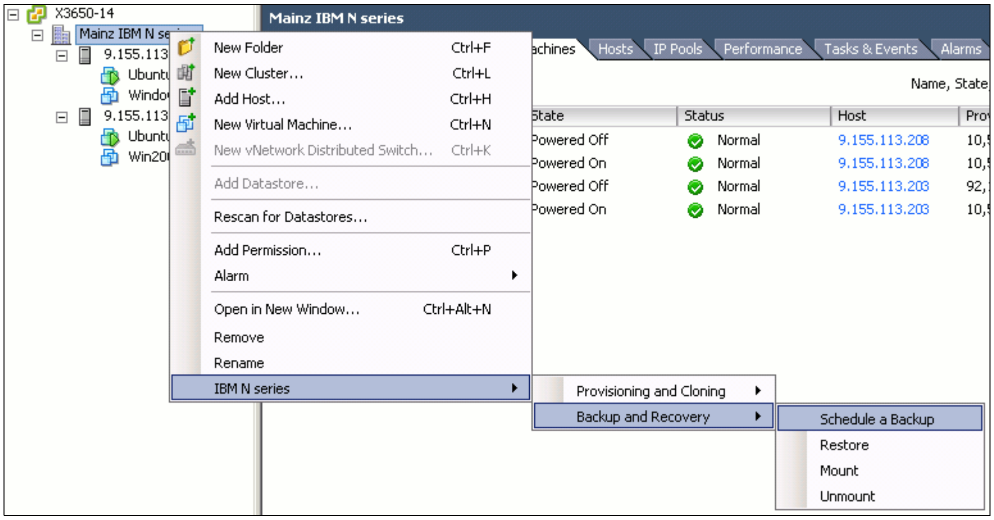
Name:	Ubuntu backup
Description:	a daily backup
Perform VMware consistency snapshot:	Yes
Perform this backup:	Every day at 21:30 starting 12/8/2011
Backup retention:	Maximum of 7 days
Email notification will be sent on:	Never

☑ Run Job Now

Figure 15-20 Revise scheduled backup job

Datacenter backup

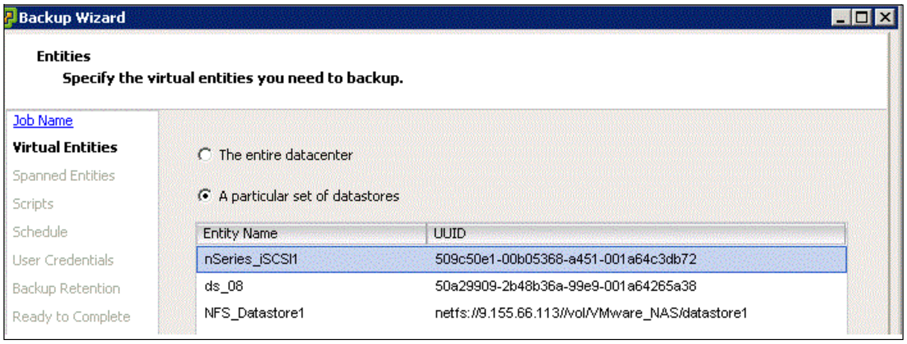
Alternatively, you can also select to back up the whole datacenter as shown in Figure 15-21. Some options are then added to the previously described process.



State	Status	Host	Pro
Powered Off	Normal	9.155.113.208	10,
Powered On	Normal	9.155.113.208	10,
Powered Off	Normal	9.155.113.203	92,
Powered On	Normal	9.155.113.203	10,

Figure 15-21 Datacenter backup

The backup wizard adds the option to select the whole datacenter of backup individual datastores as displayed in Figure 15-22.



Entities

Specify the virtual entities you need to backup.

○ The entire datacenter

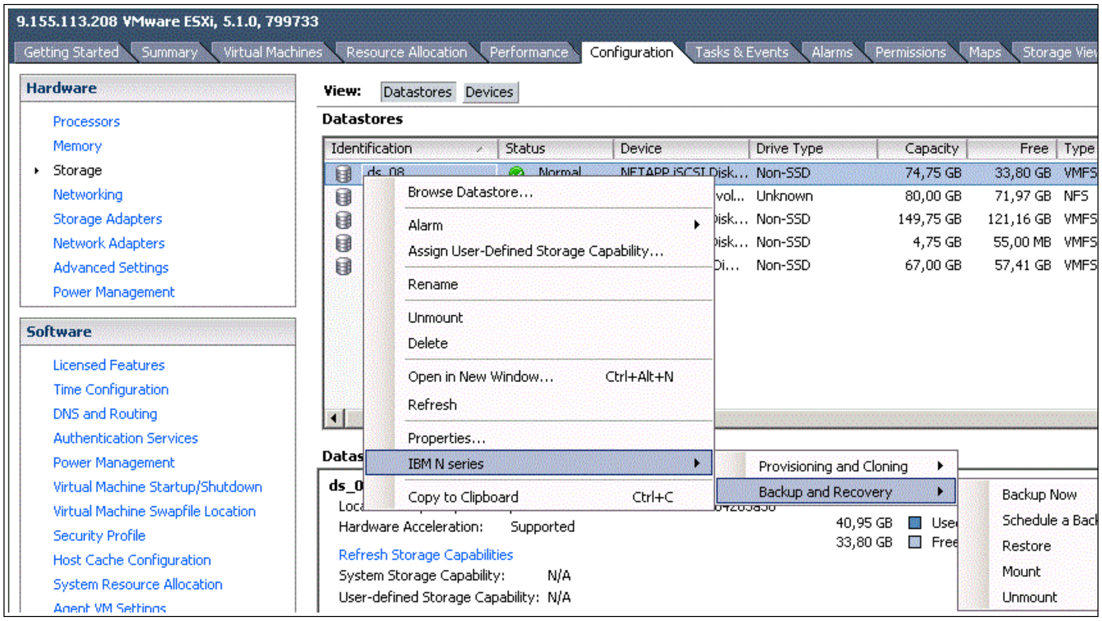
● A particular set of datastores

Entity Name	UUID
nSeries_iSCSI1	509c50e1-00b05368-a451-001a64c3db72
ds_08	50a29909-2b48b36a-99e9-001a64265a38
NFS_Datastore1	netfs://9.155.66.113//vol/VMware_NAS/datastore1

Figure 15-22 Datacenter backup options

Datastore backup

Alternatively, you can also select to back up an individual datastore as shown in Figure 15-23. Some options are then added to the previously described process.



Identification	Status	Device	Drive Type	Capacity	Free	Type
ds_08	Normal	NETAPP iSCSI Disk...	Non-SSD	74,75 GB	33,80 GB	VMFS
		vol...	Unknown	80,00 GB	71,97 GB	NFS
		Disk...	Non-SSD	149,75 GB	121,16 GB	VMFS
		Disk...	Non-SSD	4,75 GB	55,00 MB	VMFS
		Di...	Non-SSD	67,00 GB	57,41 GB	VMFS

Hardware Acceleration: Supported

Refresh Storage Capabilities

System Storage Capability: N/A

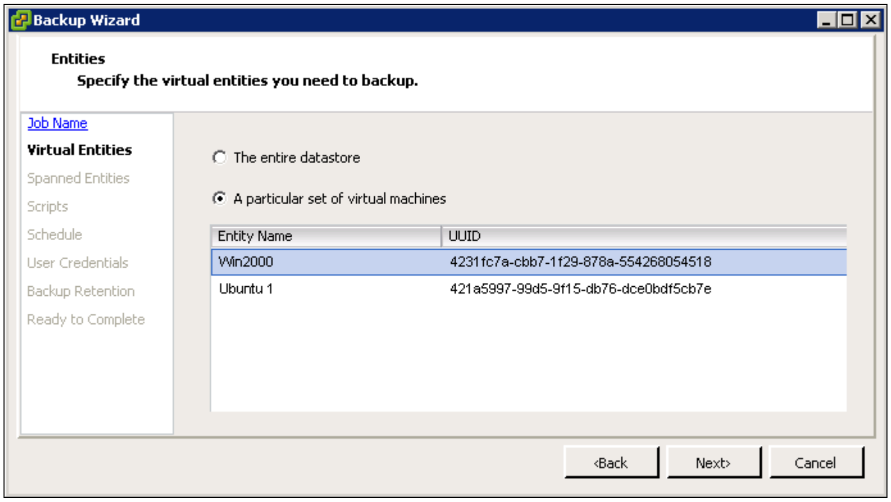
User-defined Storage Capability: N/A

40,95 GB Used

33,80 GB Free

Figure 15-23 Datastore backup

The backup wizard adds the option to select the whole datastore of backup individual datastores as displayed in Figure 15-24.



○ The entire datastore

● A particular set of virtual machines

Entity Name	UUID
Win2000	4231fc7a-cbb7-1f29-878a-554268054518
Ubuntu 1	421a5997-99d5-9f15-db76-dce0bdf5cb7e

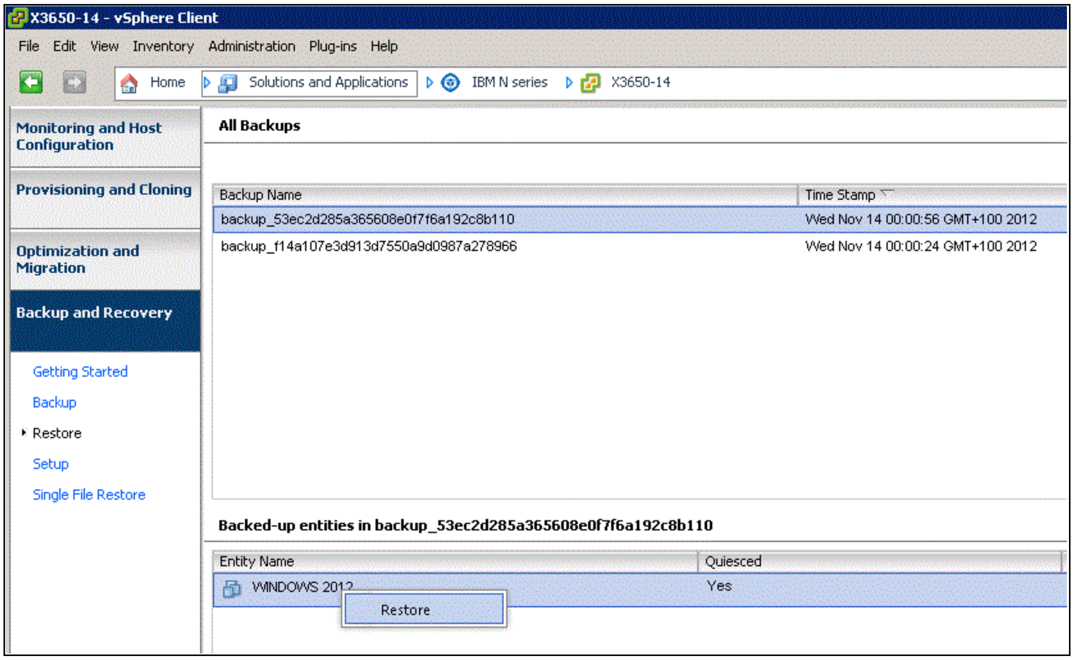
Figure 15-24 Datastore backup options

15.7.4 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 15-25. Right-click the object that you want to restore.


X3650-14 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Solutions and Applications
IBM N series
X3650-14
Monitoring and Host Configuration
Provisioning and Cloning
Optimization and Migration
Backup and Recovery
Getting Started
Backup
Restore
Setup
Single File Restore
Restore

All Backups

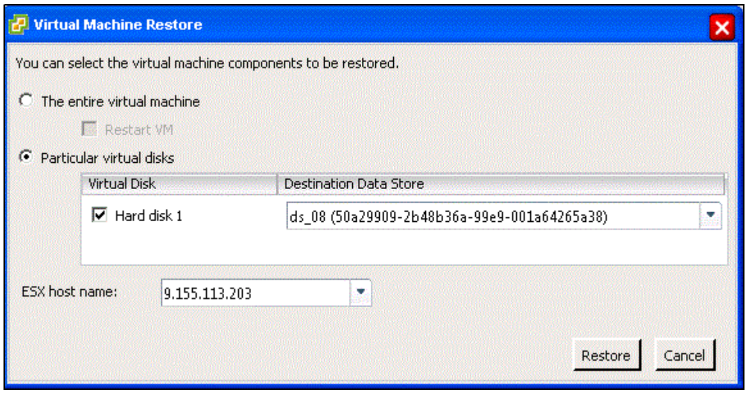
Backup Name	Time Stamp
backup_53ec2d285a365608e0f7f6a192c8b110	Wed Nov 14 00:00:56 GMT+100 2012
backup_f14a107e3d913d7550a9d0987a278966	Wed Nov 14 00:00:24 GMT+100 2012

Backed-up entities in backup_53ec2d285a365608e0f7f6a192c8b110

Entity Name	Quiesced
WINDOWS 2012	Yes

Figure 15-25 Restore options

You can also select whether you want to restore the entire virtual machine or individual virtual disks, as shown in Figure 15-26. Furthermore, you can select the original or a new location.



You can select the virtual machine components to be restored.

○ The entire virtual machine

□ Restart VM

● Particular virtual disks

Virtual Disk	Destination Data Store
☑ Hard disk 1	ds_08 (50a29909-2b48b36a-99e9-001a64265a38)

ESX host name: 9.155.113.203

Figure 15-26 VSC enhanced restore options

15.7.5 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

15.8 Provisioning and cloning

This section provide information and examples of the Provisioning and Cloning functions integrated in VSC.

15.8.1 Features and functions

The provisioning features require at 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 or later
  - Citrix XenDesktop 4.0 and 5.0 or later

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

15.8.2 Provision datastores

With the Provisioning and Cloning feature of the VSC 4.1, 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:

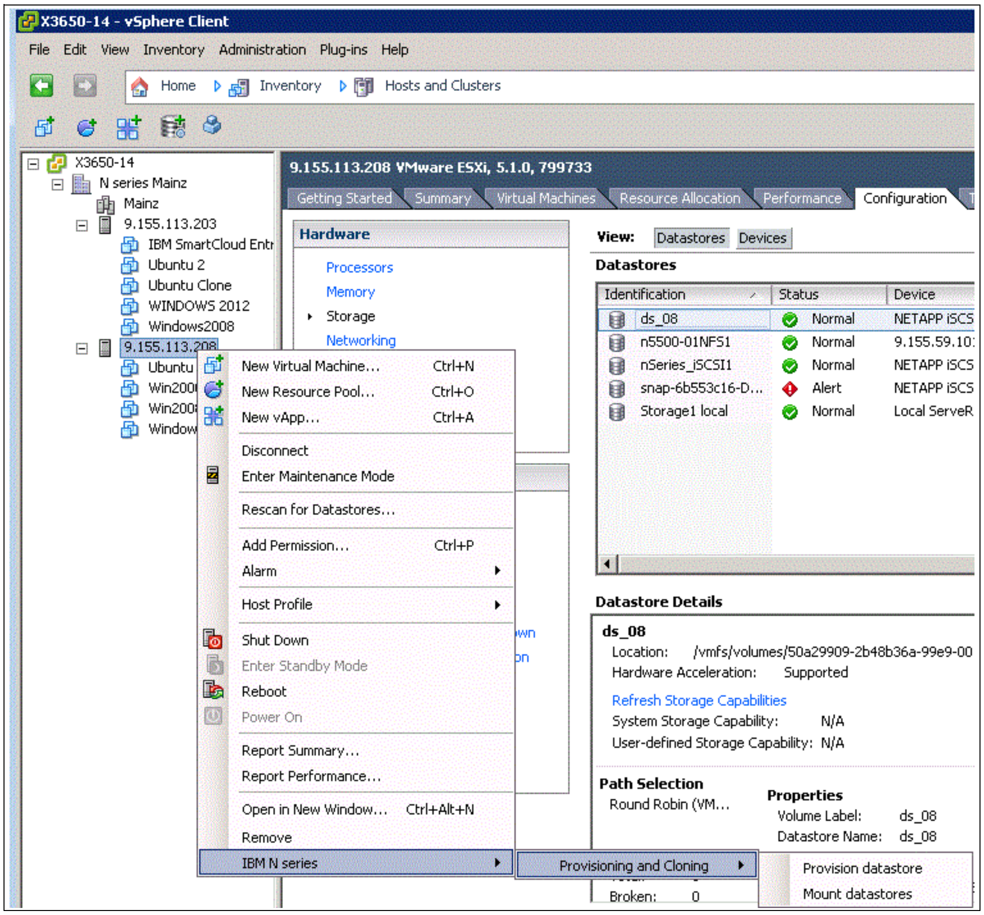
- Creating initiator groups
- Enabling ALUA
- Applying LUN masking
- Applying path selection policies
- Formatting the LUN with VMFS

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 15-27).



Datastores

Identification	Status	Device
ds_08	Normal	NETAPP iSCS
n5500-01NFS1	Normal	9.155.59.10:
nSeries_iSCSI1	Normal	NETAPP iSCS
snap-6b553c16-D...	Alert	NETAPP iSCS
Storage1 local	Normal	Local ServeR

Datastore Details

ds_08
Location: /vmfs/volumes/50a29909-2b48b36a-99e9-00
Hardware Acceleration: Supported
Refresh Storage Capabilities
System Storage Capability: N/A
User-defined Storage Capability: N/A

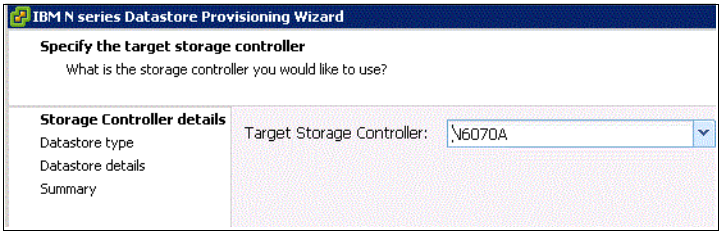
Path Selection
Round Robin (VM...

Properties
Volume Label: ds_08
Datastore Name: ds_08

Broken: 0

Figure 15-27 Provision a datastore

2. Next specify the N series system to use (see Figure 15-28).

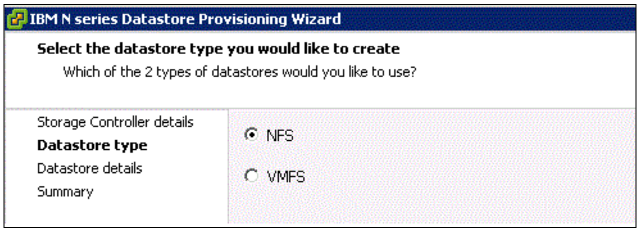

IBM N series Datastore Provisioning Wizard
Storage Controller details
Datastore type
Datastore details
Summary

Specify the target storage controller
What is the storage controller you would like to use?

Target Storage Controller: N6070A

Figure 15-28 Select storage controller for provisioning

3. In the following window, select the protocol to use. Here we only have NFS available, as shown in Figure 15-29.



IBM N series Datastore Provisioning Wizard

Select the datastore type you would like to create

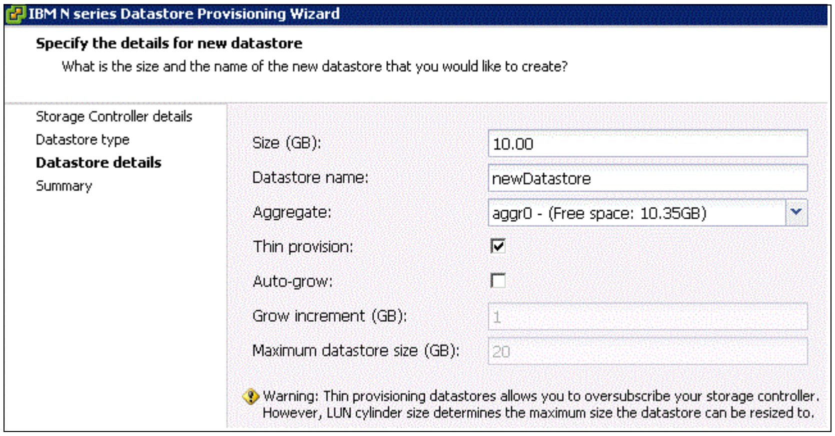
Which of the 2 types of datastores would you like to use?

● NFS

○ VMFS

Figure 15-29 Specify datastore type

4. Now specify the new datastore details (see Figure 15-30).



IBM N series Datastore Provisioning Wizard

Specify the details for new datastore

What is the size and the name of the new datastore that you would like to create?

Size (GB): 10.00

Datastore name: newDatastore

Aggregate: aggr0 - (Free space: 10.35GB)

Thin provision: ☑

Auto-grow: □

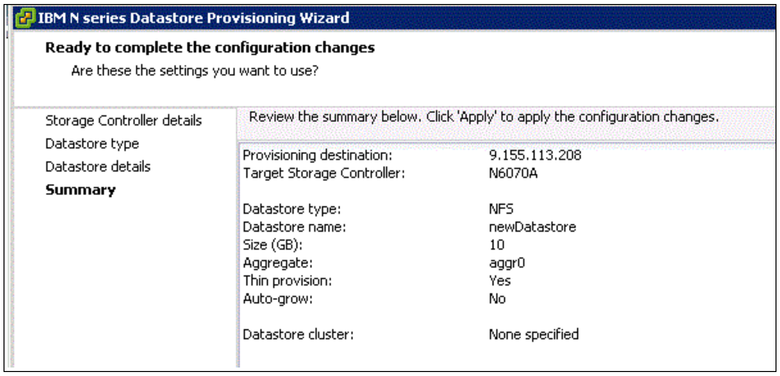
Grow increment (GB): 1

Maximum datastore size (GB): 20

Warning: Thin provisioning datastores allows you to oversubscribe your storage controller. However, LUN cylinder size determines the maximum size the datastore can be resized to.

Figure 15-30 New datastore details

5. Before applying your selection, verify the information as shown in Figure 15-31.


IBM N series Datastore Provisioning Wizard
Storage Controller details
Datastore type
Datastore details
Summary

Ready to complete the configuration changes

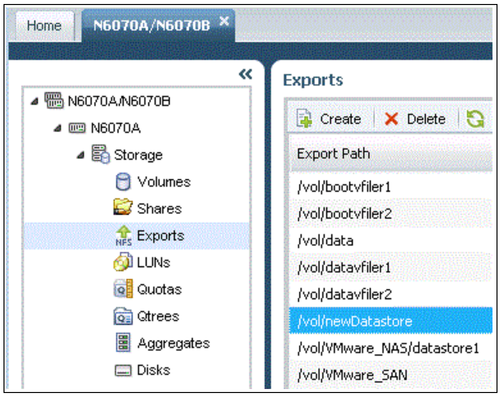
Are these the settings you want to use?

Review the summary below. Click 'Apply' to apply the configuration changes.

```
Provisioning destination:        9.155.113.208
Target Storage Controller:       N6070A

Datastore type:                  NFS
Datastore name:                  newDatastore
Size (GB):                       10
Aggregate:                       aggr0
Thin provision:                  Yes
Auto-grow:                       No

Datastore cluster:               None specified
```

Figure 15-31 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 15-32 shows System Manager access and the NFS exports.



Export Path
/vol/bootvfiler1
/vol/bootvfiler2
/vol/data
/vol/datavfiler1
/vol/datavfiler2
/vol/newDatastore
/vol/VMware_NAS/datastore1
/vol/VMware_SAN

Figure 15-32 Verify NFS exports

15.8.3 Managing deduplication

Deduplication eliminates redundant objects on a selected datastore and only references the original object. Figure 15-33 shows how VSC is able to manage deduplication for each individual datastore.

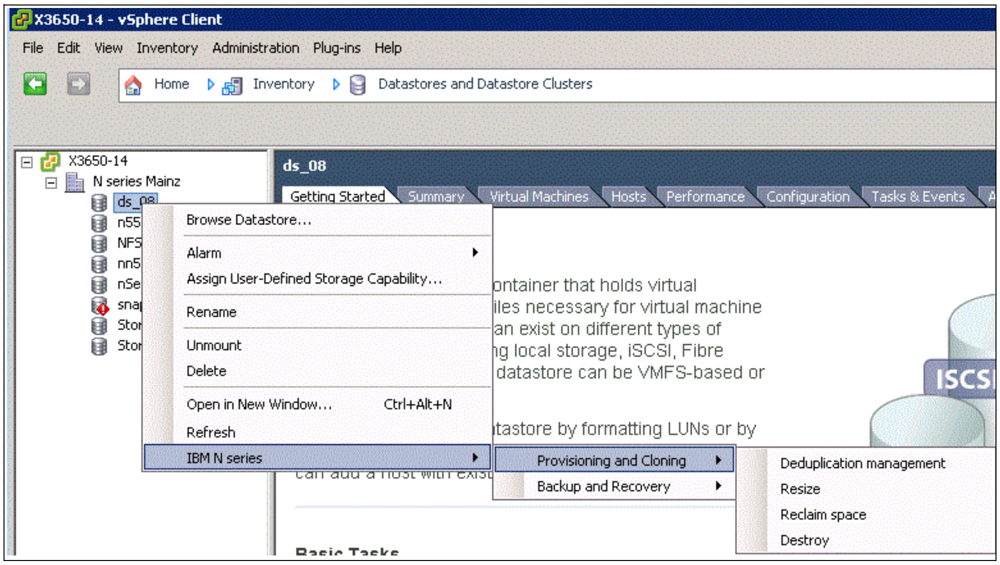
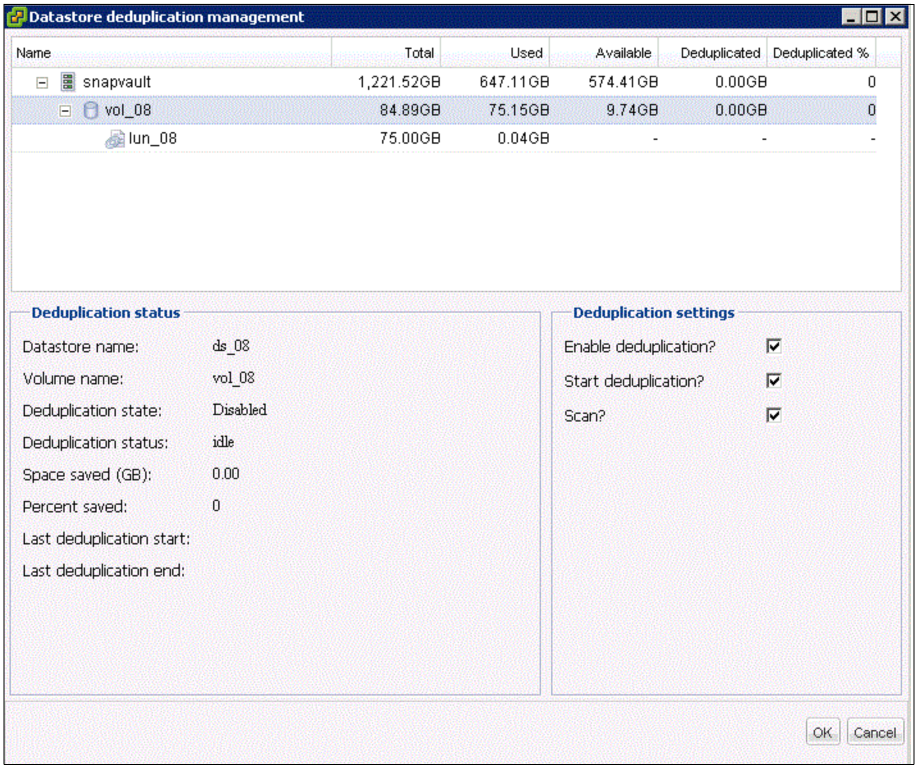

X3650-14 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Datastores and Datastore Clusters
X3650-14
N series Mainz
ds_08
n55
NFS
nn5
nSe
snap
Stor
Stor
ds_08
Getting Started
Summary
Virtual Machines
Hosts
Performance
Configuration
Tasks & Events
Browse Datastore...
Alarm
Assign User-Defined Storage Capability...
Rename
Unmount
Delete
Open in New Window... Ctrl+Alt+N
Refresh
IBM N series
Provisioning and Cloning
Backup and Recovery
Deduplication management
Resize
Reclaim space
Destroy
ontainer that holds virtual
iles necessary for virtual machine
an exist on different types of
ng local storage, iSCSI, Fibre
datastore can be VMFS-based or
tastore by formatting LUNs or by
ISCSI
Basic Tasks

Figure 15-33 Managing deduplication

Possible options to use N series advanced deduplication features are displayed in Figure 15-34. Click **OK** to apply your settings.



Name	Total	Used	Available	Deduplicated	Deduplicated %
snapvault	1,221.52GB	647.11GB	574.41GB	0.00GB	0
vol_08	84.89GB	75.15GB	9.74GB	0.00GB	0
lun_08	75.00GB	0.04GB	-	-	-

Deduplication status

Datastore name:	ds_08
Volume name:	vol_08
Deduplication state:	Disabled
Deduplication status:	idle
Space saved (GB):	0.00
Percent saved:	0
Last deduplication start:	
Last deduplication end:	

Deduplication settings

Enable deduplication? ☑

Start deduplication? ☑

Scan? ☑

Figure 15-34 Manage deduplication features

15.8.4 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 15-35) or template and select **N series** → **Provisioning and Cloning** → **Create rapid clones**.

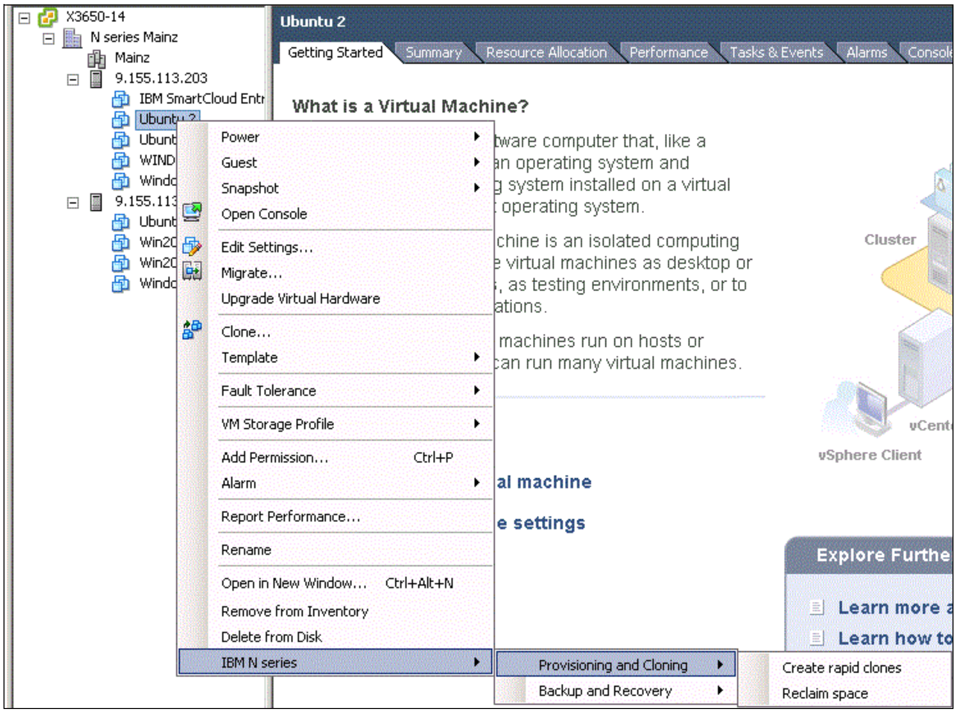
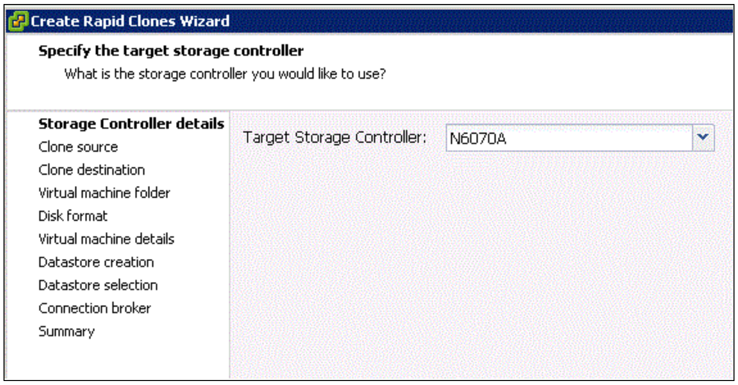


Figure 15-35 Select VM for cloning

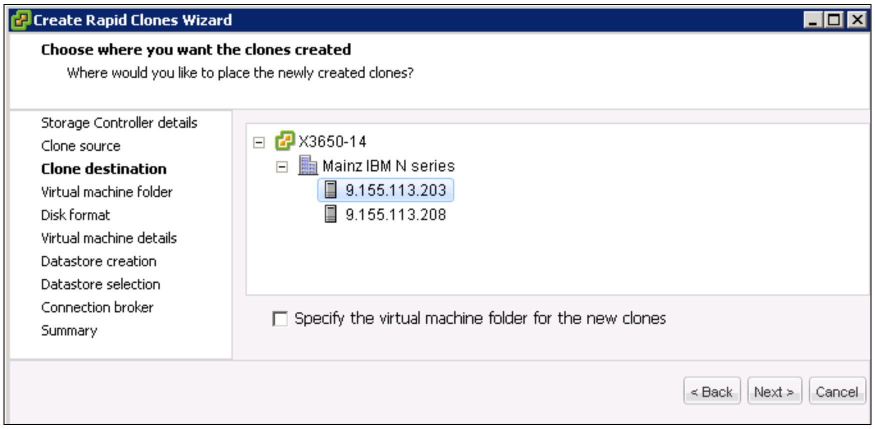
2. Next select the controller you want to use for cloning (see Figure 15-36).



Target Storage Controller: N6070A

Figure 15-36 Select controller for cloning

3. In the following window, select the destination N series system (see Figure 15-37).



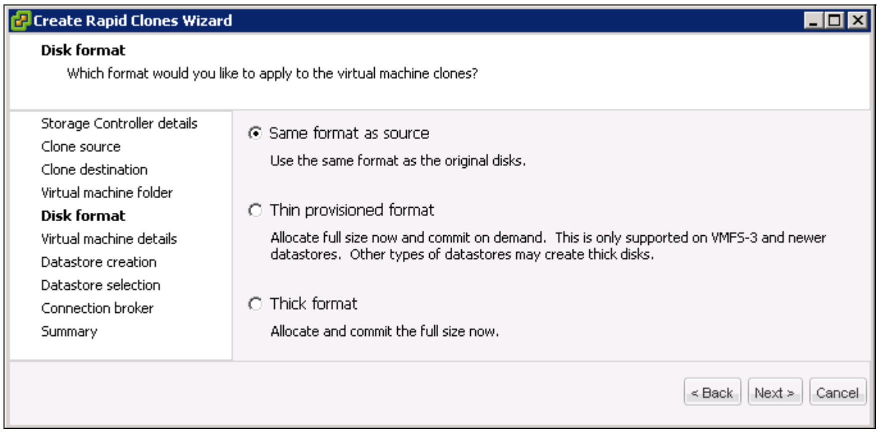
Choose where you want the clones created

Where would you like to place the newly created clones?

□ Specify the virtual machine folder for the new clones

Figure 15-37 Select clone target

4. Now specify the VM format for the clone as shown in Figure 15-38.



Disk format

Which format would you like to apply to the virtual machine clones?

● Same format as source

Use the same format as the original disks.

○ Thin provisioned format

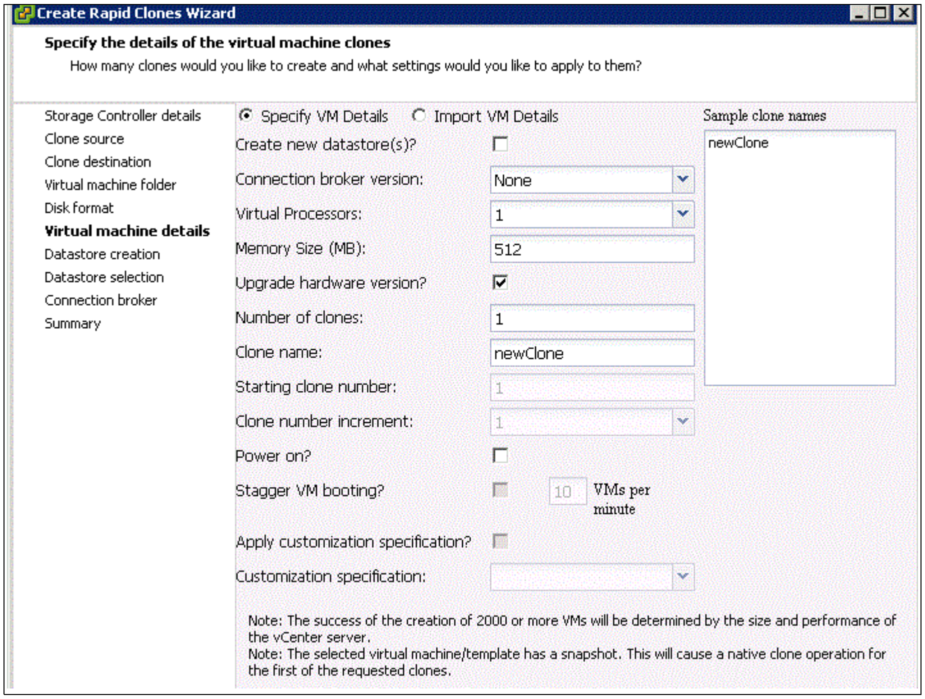
Allocate full size now and commit on demand. This is only supported on VMFS-3 and newer datastores. Other types of datastores may create thick disks.

○ Thick format

Allocate and commit the full size now.

Figure 15-38 Clone VM format

5. In the following window, specify details for the new datastores as displayed in Figure 15-39.



Create Rapid Clones Wizard

Specify the details of the virtual machine clones

How many clones would you like to create and what settings would you like to apply to them?

Storage Controller details
Clone source
Clone destination
Virtual machine folder
Disk format
Virtual machine details
Datastore creation
Datastore selection
Connection broker
Summary

● Specify VM Details ○ Import VM Details

Create new datastore(s)?	□
Connection broker version:	None
Virtual Processors:	1
Memory Size (MB):	512
Upgrade hardware version?	☑
Number of clones:	1
Clone name:	newClone
Starting clone number:	1
Clone number increment:	1
Power on?	□
Stagger VM booting?	□ 10 VMs per minute
Apply customization specification?	□
Customization specification:	

Sample clone names

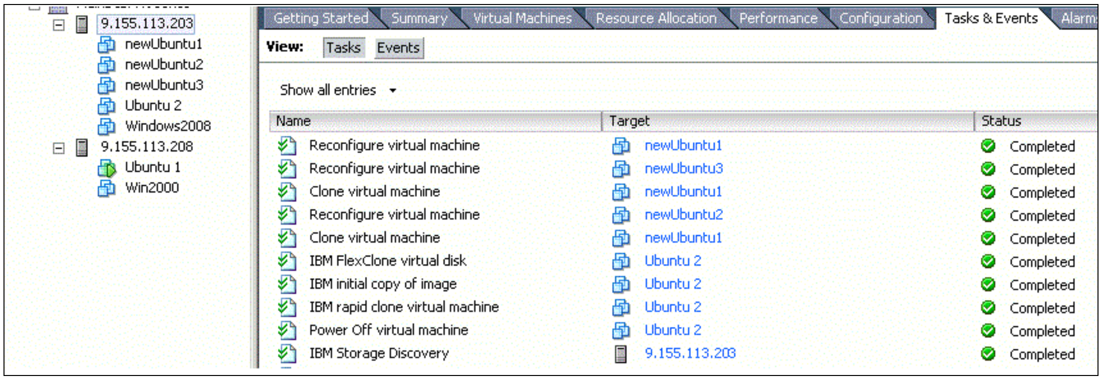
newClone

Note: The success of the creation of 2000 or more VMs will be determined by the size and performance of the vCenter server.
Note: The selected virtual machine/template has a snapshot. This will cause a native clone operation for the first of the requested clones.

Figure 15-39 Clone VM details

6. When a summary is provided, click **Apply** to execute your selection.

After successful completion of the cloning tasks, the new VMs are configured and ready for further use. Figure 15-40 shows the cloning results.



Name	Target	Status
Reconfigure virtual machine	newUbuntu1	Completed
Reconfigure virtual machine	newUbuntu3	Completed
Clone virtual machine	newUbuntu1	Completed
Reconfigure virtual machine	newUbuntu2	Completed
Clone virtual machine	newUbuntu1	Completed
IBM FlexClone virtual disk	Ubuntu 2	Completed
IBM initial copy of image	Ubuntu 2	Completed
IBM rapid clone virtual machine	Ubuntu 2	Completed
Power Off virtual machine	Ubuntu 2	Completed
IBM Storage Discovery	9.155.113.203	Completed

Figure 15-40 Clone results

15.8.5 Reclaiming space on virtual machines

You can use the Reclaim space feature to find free clusters on NTFS partitions and make them available to the operating system.

Before you begin

The Reclaim space feature allows Data ONTAP to use space freed when data is deleted in guest operating systems.

This feature has the following requirements:

- VMDKs attached to the virtual machine must be on NFS-backed datastores.

> **Tip:** The Reclaim space feature is not supported if the NFS datastore is backed by a qtree on a vFiler unit.

- VMDKs must have NTFS partitions.

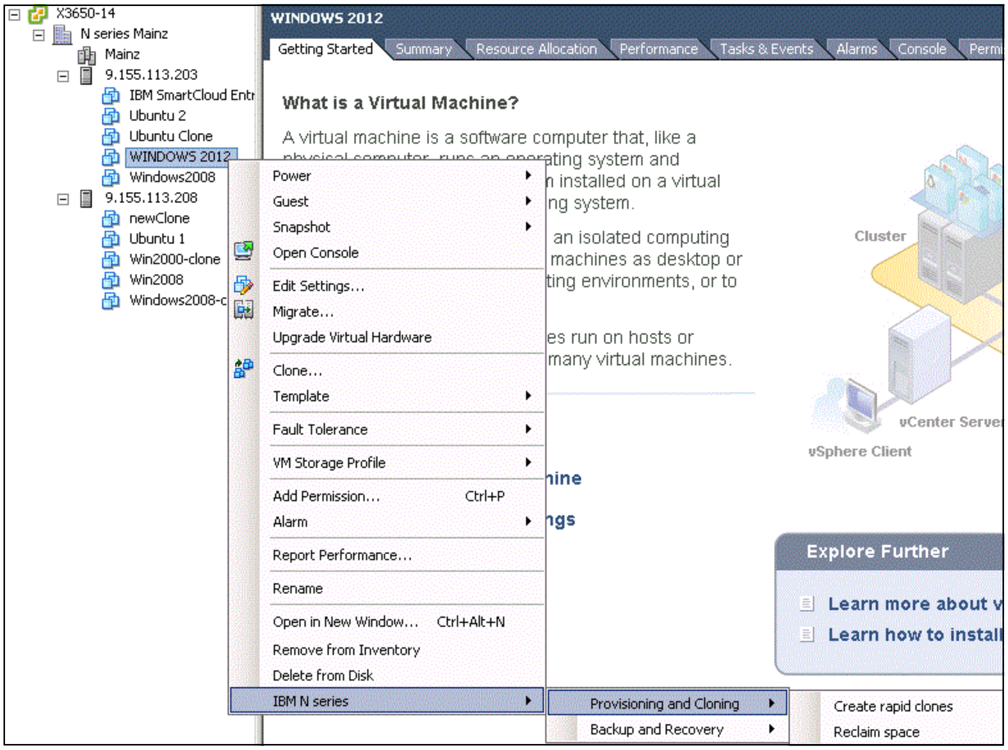
> **Tip:** If the VMDK is unpartitioned or FAT, the Provisioning and Cloning capability incorrectly lists the disk as having an NTFS partition after the task completes and displays a “Yes” in the “Has NTFS partition(s)?” column. Even though the VMDK now appears to be partitioned, it is still unpartitioned or FAT, and you cannot reclaim space on it.

- ISOs mounted to the virtual machine must be contained in an NFS datastore.
- Storage systems must be running Data ONTAP 7.3.4 or later.
- You should have the VMware guest tools installed.
- When the Reclaim space feature is running, you must not power on the virtual machine.
- You cannot use the cloning feature when the target virtual machine is being used by either the Backup and Recovery capability or the Optimization and Migration capability.

Steps

Follow these steps:

1. Right-click a datastore or virtual machine and select **IBM N series** → **Provisioning and Cloning** → **Reclaim space** (Figure 15-41).



A virtual machine is a software computer that, like a physical computer, runs an operating system and ... n installed on a virtual ... ng system. ... an isolated computing ... machines as desktop or ... ting environments, or to ... es run on hosts or ... many virtual machines.

Figure 15-41 VM reclaim space

2. Click **OK**.

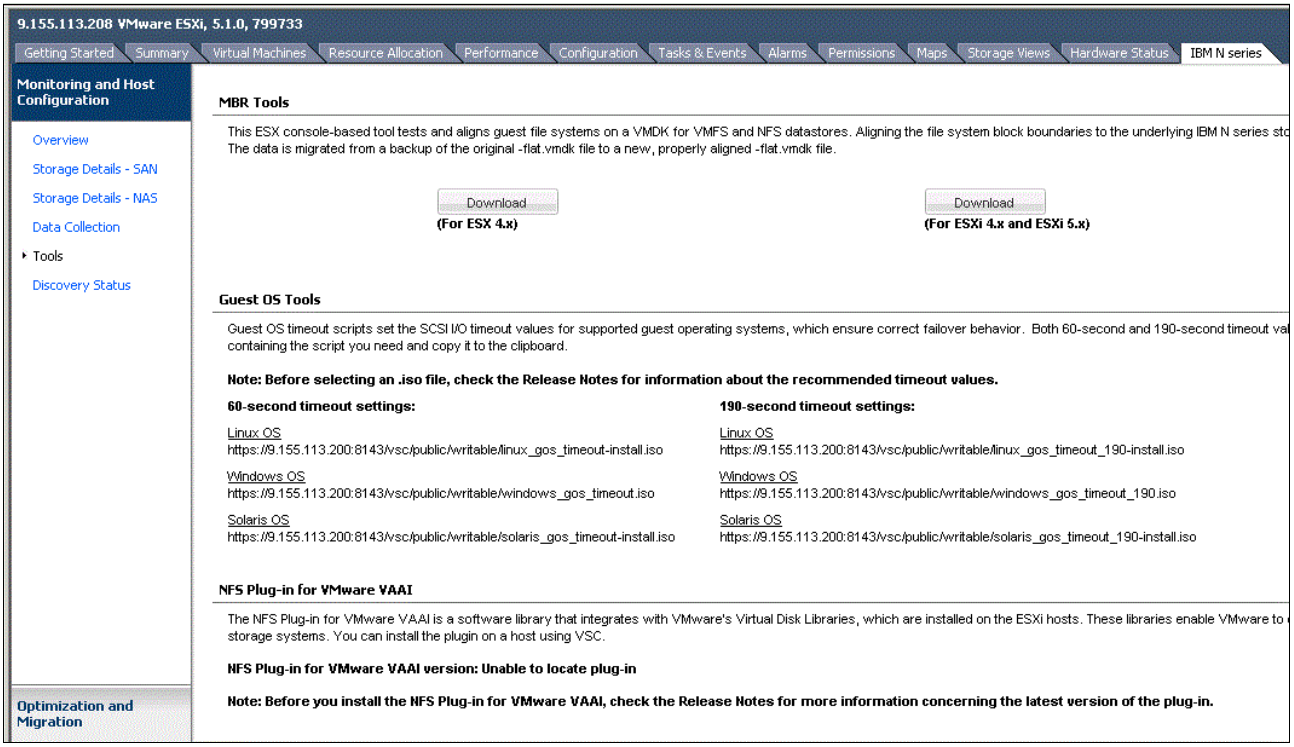
If the virtual machine is powered on, the Reclaim space feature powers it off. After the process completes, the Reclaim space feature returns the virtual machine to its previous state.

Tip: If you are using this feature when the virtual machine is powered on, make sure you have the guest operating system tools installed. Without these tools, the Reclaim space feature does not work when it has to power down the virtual machine.

If you do not want to install these tools, then you should power down the virtual machine before running the Reclaim space feature.

15.9 Optimum VM availability

The Monitoring and Host Configuration capability includes tools for detecting and correcting misaligned disk partitions and for setting virtual machine timeouts as shown in Figure 15-42.



MBR Tools

This ESX console-based tool tests and aligns guest file systems on a VMDK for VMFS and NFS datastores. Aligning the file system block boundaries to the underlying IBM N series sto
The data is migrated from a backup of the original -flat.vmdk file to a new, properly aligned -flat.vmdk file.

(For ESX 4.x)

(For ESXi 4.x and ESXi 5.x)

Guest OS Tools

Guest OS timeout scripts set the SCSI I/O timeout values for supported guest operating systems, which ensure correct failover behavior. Both 60-second and 190-second timeout val
containing the script you need and copy it to the clipboard.

Note: Before selecting an .iso file, check the Release Notes for information about the recommended timeout values.

60-second timeout settings:

Linux OS
https://9.155.113.200:8143/vsc/public/writable/linux_gos_timeout-install.iso

Windows OS
https://9.155.113.200:8143/vsc/public/writable/windows_gos_timeout.iso

Solaris OS
https://9.155.113.200:8143/vsc/public/writable/solaris_gos_timeout-install.iso

190-second timeout settings:

Linux OS
https://9.155.113.200:8143/vsc/public/writable/linux_gos_timeout_190-install.iso

Windows OS
https://9.155.113.200:8143/vsc/public/writable/windows_gos_timeout_190.iso

Solaris OS
https://9.155.113.200:8143/vsc/public/writable/solaris_gos_timeout_190-install.iso

NFS Plug-in for VMware VAAI

The NFS Plug-in for VMware VAAI is a software library that integrates with VMware's Virtual Disk Libraries, which are installed on the ESXi hosts. These libraries enable VMware to
storage systems. You can install the plugin on a host using VSC.

NFS Plug-in for VMware VAAI version: Unable to locate plug-in

Note: Before you install the NFS Plug-in for VMware VAAI, check the Release Notes for more information concerning the latest version of the plug-in.

Figure 15-42 VSC tools

Tip: The Optimization and Migration capability of VSC allows you to perform online alignments on VMFS-based datastores without having to take your VM down. This capability also lets you review the alignment status of VMs and migrate groups of VMs.

15.9.1 Optimizing VM SCSI BUS

One of the components of the VSC is the GOS timeout scripts. These scripts are a collection of ISO images that can be mounted by a VM to configure its local SCSI to values that are optimal for running in a virtual infrastructure.

Installing GOS scripts

The ISO images of the guest operating system (GOS) scripts are loaded on the VSC for VMware vSphere server. Mount and run them from the vSphere Client to set the storage timeouts for virtual machines.

Before you begin

The virtual machine must be running.

The CD-ROM must already exist in the virtual machine or it must be added.

The script must be installed from the copy of the VSC for VMware vSphere registered to the vCenter Server that manages the VM.

Steps

1. Open the vSphere Client and log into your vCenter Server.
2. Select a **Datacenter** in the Inventory panel, and then select the **IBM N series** tab.
3. In the Monitoring and Host Configuration capability, select the **Tools** panel.
4. Under **Guest OS Tools**, right-click the link to the ISO image for your guest operating system version and select **Copy to clipboard**.
5. In the vSphere Client, select the desired VM and click the **CD/DVD Connections** icon.
6. Select **CD/DVD Drive 1** > **Connect to ISO image on local disk**.
7. Paste the link you copied into the **File Name** field and then click **Open**.

If you receive an authorization error, be sure you select the IBM N series tab and click **Yes** to proceed if a security certificate warning is displayed.

Also, be sure that the link you are using is from the copy of the VSC for VMware vSphere running on the vCenter Server that manages the VM.

After you finish

Log on to the VM and run the script to set the storage timeout values

15.9.2 Optimal storage performance

VMs store their data on virtual disks. Similar to physical disks, these virtual disks contain storage partitions and file systems, which are created by the guest operating system of the VM. To provide optimal disk I/O within the VM, you must align the partitions of the virtual disks to the block boundaries of VMFS and the block boundaries of the storage array. Failure to align all three of these items results in a dramatic increase of I/O load on a storage array and negatively affects the performance of all VMs being served on the array.

IBM, VMware, other storage vendors, and VMware partners recommend aligning the partitions of VMs and the partitions of VMFS datastores to the blocks of the underlying storage array.

Datastore alignment

N series systems automate the alignment of VMFS with iSCSI, FC, and FCoE LUNs. This task is automated during the LUN provisioning phase of creating a datastore when you select the LUN type “VMware” for the LUN. Customers deploying VMware over NFS do not need to align the datastore. With any type of datastore, VMFS or NFS, the virtual disks contained within should have the partitions aligned to the blocks of the storage array.

VM partition alignment

When aligning the partitions of virtual disks for use with N series systems, the starting partition offset must be divisible by 4,096. For example, the starting partition offset for Microsoft Windows 2000, 2003, and XP operating systems is 32,256. This value does not align to a block size of 4,096.

Virtual machines running a clean installation of Microsoft Windows 2008, Windows 7, or Windows Vista operating systems automatically have their starting partitions set to 1,048,576. By default, this value does not require any adjustments.

> **Tip:** If your Windows 2008 or Windows Vista VMs were created by upgrading an earlier version of Microsoft Windows to one of these versions, then it is highly probable that these images require partition alignment.

15.9.3 VM partition alignment

Storage alignment is critical, so aligning the file system within the VMs to the storage array is very important. This process should not be considered optional. Misalignment at a high level results in decreased usage.

Issues with partition alignment

Failure to align the file systems results in a significant increase in storage array I/O to meet the I/O requirements of the hosted VMs. Customers might notice this impact when:

- Running high-performance applications
- Achieving less than impressive storage savings with deduplication
- Perceiving a need to upgrade storage array hardware

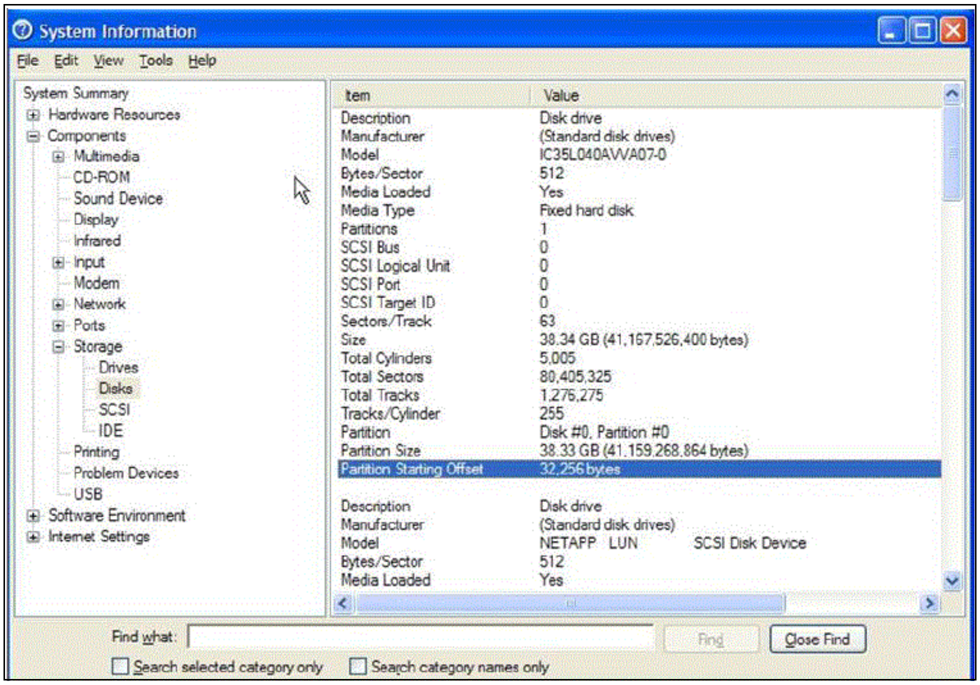
The reason for these types of issues is misalignment results in every I/O operation executed within the VM to require multiple I/O operations on the storage array.

Simply put, you can save your company a significant amount of capital expenditures by optimizing the I/O of your VMs.

Identifying partition alignment

To verify the starting partition offset for a VM based on Windows, complete the following steps:

1. Log in to the VM.
2. Run the system information utility (or `msinfo32`) to find the starting partition offset setting.
3. To run `msinfo32`, click **Start** > **All Programs** > **Accessories** > **System Tools** > **System Information** (Figure 15-43 on page 271).



Item	Value
Description	Disk drive
Manufacturer	(Standard disk drives)
Model	IC35L040AVVA07-0
Bytes/Sector	512
Media Loaded	Yes
Media Type	Fixed hard disk
Partitions	1
SCSI Bus	0
SCSI Logical Unit	0
SCSI Port	0
SCSI Target ID	0
Sectors/Track	63
Size	38.34 GB (41,167,526,400 bytes)
Total Cylinders	5,005
Total Sectors	80,405,325
Total Tracks	1,276,275
Tracks/Cylinder	255
Partition	Disk #0, Partition #0
Partition Size	38.33 GB (41,159,268,864 bytes)
Partition Starting Offset	32,256 bytes
Description	Disk drive
Manufacturer	(Standard disk drives)
Model	NETAPP LUN SCSI Disk Device
Bytes/Sector	512
Media Loaded	Yes

Figure 15-43 System information

15.9.4 N series MBR Tools: Identification of partition alignment status

IBM N series systems provides a tool, MBRScan, that runs on an ESX host and can identify if partitions are aligned with Windows and Linux VMs running within VMFS and NFS datastores. MBRScan runs against the virtual disk files that compose a VM. Although this process only requires a few seconds per VM to identify and report on the status of the partition alignment, each VM must be powered off. For this reason, it might be easier to identify the file system alignment from within each VM, because this action is nondisruptive.

MBRScan is an integrated component of the VSC.

Corrective actions for VMs with misaligned partitions

After you identify that your VMs have misaligned partitions, we recommend correcting the partitions in your templates as the first corrective action. This step makes sure that any newly created VM is properly aligned and does not add to the I/O load on the storage array.

Correcting partition misalignment with N series MBR Tools

As part of the VSC tools, IBM N series systems provides a tool, MBRAlign, that runs on an ESX host and can correct misaligned primary and secondary master boot record-based partitions for guest operating systems. When using MBRAlign, the VM that is undergoing the corrective action must be powered off.

MBRAlign provides flexible repair options. For example, it can be used to migrate and align a virtual disk as well as change the format from a thin to thick vmdk. We highly recommend creating a Snapshot copy before executing MBRAlign. This Snapshot copy can be safely discarded after a VM has been corrected, powered on, and the results have been verified.

You must download these tools before you can use them. There is a set of tools for ESX hosts and one for ESXi hosts. You must download the correct tool set for your hosts. MBRAlign can be obtained from the Tools Download link in the VSC.

Enabling the ESXi secure shell

When you are using ESXi, it is a good practice to enable the Secure Shell (SSH) protocol before you download the MBR tools. That way you can use the `scp` command if you need to copy the files.

Before you begin

ESXi does not enable this shell by default.

Steps

1. From an ESXi host, press the key combination **ALT F2** to access the Direct Console User Interface (DCUI) panel.
2. Press the **F2** function key to get to the Customize System panel.
3. Go to **Troubleshooting Options**.
4. Press **Enter** at the Enable SSH prompt.
5. Press **Enter** at the Modify ESX Shell timeout prompt.
6. Disable the timeout by setting the value to zero (0) and pressing **Enter**.
7. Go to **Restart Management Agents** and press **Enter**.
8. Press **F11**.

Downloading and installing MBR tools for ESXi hosts

If you have an ESXi host, you must download and install the version of the MBR (master boot record) tools for ESXi. The MBR tools enable you to detect and correct misaligned disk partitions for guest operating systems. These tools must be installed and run directly on the ESXi host. Before you install them, you must extract them from the .tar file into the root directory on the ESXi host.

Before you begin

You must be able to open a console connection to the ESXi host.

> **Tip:** The MBR tools can only be used when the virtual machine (VM) is powered off. If you want to perform online alignments on VMFS-based datastores without having to take your VM down, you can use the Optimization and Migration capability. In that case, you do not need to download the MBR tools.

Steps

Follow these steps:

1. Open the vSphere Client and log into your vCenter Server.
2. Select a Datacenter in the **Inventory** panel, and then select the **IBM N series** tab.
3. In the Monitoring and Host Configuration capability, select the **Tools** panel.
4. Under **MBR Tools**, click the **Download (For ESXi 4.x and ESXi 5.x)** button.

   Make sure you download the MBR Tools for ESXi. If you download the wrong MBR tools file, the tools will **not** work.
5. When the File Download dialog is displayed, click **Save**.
6. **(ESXi 4.x)** If you are using ESXi 4.x, manually enable the ESXi shell and SSH so that you can use the scp command to copy the files to the correct directories if needed.

ESXi 4.x does not enable the ESXi shell and SSH by default. You can enable these options from the physical host or from the vCenter. The following steps enable these options from the vCenter.

Tip: vCenter creates a configuration alert for each ESXi host that has the options enabled.

To enable the ESXi shell, perform the following steps:

- From vCenter, highlight the appropriate ESXi host.
- Go to the **Configuration** Tab.
- In the left pane under **Software**, select **Security Profile**.
- Select **Properties** from the **Services** pane.
- Highlight the **ESXi Shell** service and select **Options**.
- Select **Start and Stop with Host**.
- Click **Start**.

To enable the ESXi SSH, perform the following steps:

- From vCenter, highlight the appropriate ESXi host.
- Go to the **Configuration** Tab.
- In the left pane under **Software**, select **Security Profile**.
- Select **Properties** from the **Services** pane.
- Highlight the **SSH service** and select **Options**.
- Select **Start and Stop with Host**.
- Click **Start.**

7. Copy the MBR tools for ESXi file to the root (/) directory of the ESXi host. If you are using ESXi 4.x, use the Troubleshooting Console. If you are using ESXi 5.x, use the Technical Service Console.

You might need to open ESXi firewall ports to enable copying the tools to the host.

Tip: The MBR tools libraries must be located in specific directories on the host. Be sure to download the file to the root directory of the ESXi host.

8. Extract the files by entering the following command:

```
tar -zxf mbrtools_esxi.tgz
```

If you did not download the file to the root directory, you must manually move the files to that directory.

Tip: ESXi does not support -P with the tar command.

After you finish

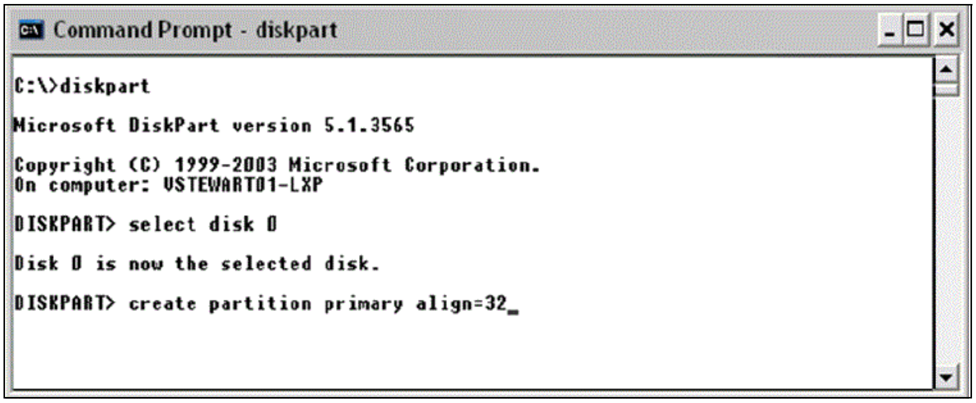
Run the `mbralign` tool to check and fix the partition alignment.

Linux VMs that boot using the GRUB boot loader require the following steps after MBRAlign has been run.

1. Connect a Linux CD or CDROM ISO image to the Linux VM.
2. Boot the VM.
3. Select to boot from the CD.
4. Execute GRUB setup to repair the boot loader, when appropriate.

Creating properly aligned partitions for new VMs

Virtual disks can be formatted with the correct offset at the time of creation by simply booting the VM before installing an operating system and manually setting the partition offset. For Windows guest operating systems, consider using the Windows Preinstall Environment boot CD or the alternative “live DVD” tools. To set up the starting offset, complete the following steps (Figure 15-44).



```
C:\>diskpart

Microsoft DiskPart version 5.1.3565

Copyright (C) 1999-2003 Microsoft Corporation.
On computer: VSTEWART01-LXP

DISKPART> select disk 0

Disk 0 is now the selected disk.

DISKPART> create partition primary align=32_
```

Figure 15-44 Running diskpart to set a proper starting partition offset

1. Boot the VM with the Microsoft WinPE CD.
2. Select **Start**, select **Run**, and enter `diskpart`
3. Enter `select disk 0`
4. Enter `create partition primary align=32`
5. Reboot the VM with the WinPE CD.
6. Install the operating system as normal.

You can also create properly aligned VMDKs with `fdisk` from an ESX console session.

15.9.5 Windows VM file system performance

If your VM is not acting as a file server, consider implementing the following change to your VMs, which disables the access time updates process in the Microsoft Windows NT File System (NTFS). This change reduces the amount of IOPS occurring within the file system.

Reducing IOPS in the file system

To make the proposed change, complete the following steps:

1. Log into a Windows VM.
2. Click **Start** → **Run**, and enter CMD.
3. Enter:

   ```
   fsutil behavior set disablelastaccess 1
   ```

Disk defragmentation utilities

VMs stored on N series storage arrays should not use disk defragmentation utilities because the WAFL file system is designed to optimally place and access data at a level below the guest operating system (GOS) file system.

15.10 VSC commands

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:

- VSC 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**.

15.11 Scripting

VSC provides users the ability to run pre, post, and failure backup phase scripts 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 <VSC Installation>\smvi\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 15-17 on page 253. The UI lists all files found in the `<VSC Installation>\smvi\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 `<VSC Installation>\smvi\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.

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. Note that some publications referenced in this list might be available in softcopy only.

- *IBM System Storage N series Hardware Guide*, SG24-7840
- *IBM System Storage N series Software Guide*, SG24-7129
- *N series Reference Architecture for Virtualized Environments,* REDP-4865-00
- *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
- *IBM System Storage N series and VMware vSphere Storage Best Practices,* SG24-7871
- *IBM System Storage N series with VMware vSphere 4.1*, SG24-7636
- *IBM System Storage N series with VMware vSphere 4.1 using Virtual Storage Console 2*, REDP-4863
- *Designing an IBM Storage Area Network*, SG24-5758
- *Introduction to Storage Area Networks and System Networking*, SG24-5470
- *IP Storage Networking: IBM NAS and iSCSI Solutions*, SG24-6240
- *Storage and Network Convergence Using FCoE and iSCSI,* SG24-7986
- *IBM Data Center Networking: Planning for Virtualization and Cloud Computing*, SG24-7928.

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

© Copyright IBM Corp. 2013. All rights reserved.

Other publications

These publications 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

- IBM System Storage N series Machine Types and Models (MTM) Cross Reference:

  http://www-304.ibm.com/support/docview.wss?uid=ssg1S7001844

- IBM N series to NetApp Machine type comparison table:

  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/TD105042

- Interoperability matrix:

  http://www-304.ibm.com/support/docview.wss?uid=ssg1S7003897

- VMware documentation:

  http://www.vmware.com/support/pubs/

- VMware vSphere 5 documentation:

  http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html
  http://pubs.vmware.com/vsphere-50/index.jsp

- VMware Capacity Planner:

  http://www.vmware.com/products/capacity-planner/

- VMware vSphere 4.1 configurations maximum:

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

- VMware vCloud suite:

  http://www.vmware.com/products/datacenter-virtualization/vcloud-suite/overview.html

Online resources

These websites are also relevant as further information sources:

- IBM NAS support website:

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

- NAS product information:

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

- IBM Integrated Technology Services:

  http://www.ibm.com/planetwide/

Help from IBM

IBM Support and downloads:

ibm.com/support

IBM Global Services:

ibm.com/services

IBM System Storage N series with VMware vSphere 5

(0.5” spine)
0.475”<->0.873”
250 <-> 459 pages

IBM System Storage N series with VMware vSphere 5

Learn how to integrate VMware vSphere 5.x 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 5.x. It explains how to use the N series with VMware vSphere 5 environments and the benefits of doing so. Examples are given on how to install and set up VMware ESXi server with the N series.

The IBM System Storage N series used as a storage foundation offers unified storage solutions that provide industry-leading technologies in the areas of storage efficiencies, instantaneous virtual machine and datastore cloning for virtual servers and virtual desktops, and virtual data center backup and business continuance solutions.

The information provided can be also be used as a foundation to create dynamic cloud solutions, making full use of underlying storage features and functions. This book provides a blueprint for how clients can create a virtualized infrastructure/storage cloud that will help to address current and future data storage business requirements.

IBM System Storage N series in conjunction with VMware vSphere 5 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.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-8110-00 ISBN 0738437832