



Руководство по наилучшим способам использования систем NetApp с VMware Virtual Infrastructure 3®

NetApp, Inc.

TR-3428

Редакция: Декабрь 2008.

M. Vaughn Stewart

Michael Slisinger

Larry Touchette

СОДЕРЖАНИЕ

Содержание	2
1. Кратко о важном.....	5
2. Варианты подключения системы хранения к VMware	6
2.1 VMFS Datastore подключенный по Fibre Channel или iSCSI	6
2.2 NAS Datastore подключенный через NFS	7
2.3 Raw Device Mapping через Fibre Channel или iSCSI	8
2.4 Таблица сравнения методов доступа к Datastore	9
3. Конфигурирование и установка NetApp FAS	11
3.1 Конфигурирование системы хранения.....	11
Защита данных с помощью RAID.....	11
Aggregates.....	11
Flexible Volumes (FlexVol)	11
LUN	12
Соглашение о порядке именования	12
4. Основы конфигурирования Virtual Infrastructure 3	13
4.1 Ограничения и рекомендации конфигурирования.....	13
Опции томов NetApp	13
RDM и ограничения на размер в VMware Cluster.....	13
Правила создания LUN для VMFS Datastores	13
Ограничения для NFS Datastore	14
Дополнительные рекомендации по NFS.....	15
Применение патчей к системе под ESX и ESXi 3.5 update 3:.....	16
Применение патчей к системе под ESX и ESXi 3.5 update 1 или update 2:	16
О системах под ESX или ESXi версий до 3.5 update 1:	17
Начальное смещение Виртуального Диска.....	17
Форматирование с правильным Partition Offsets.....	18
Оптимизация файловой системы Windows для наилучшей производительности ввода-вывода.....	19
4.2 Распределение пространства хранения.....	19
Требования VMware для Fibre Channel и iSCSI.....	19
Распределение пространства хранения на Fibre Channel и iSCSI LUN	19
4.3 Распределение пространства хранения на NFS.....	22
Хост ESX 3.5.....	25
Хост ESX 3.0.....	25
4.4 Подключение системы хранения.....	26
Подключение по Fibre Channel.....	26
Подключение по iSCSI/IP SAN	28
Подключение по NFS.....	32
Multipathing-подключение NetApp по Fibre Channel	33
Multipathing-подключение в VMware для Fibre Channel и iSCSI.....	33
Multipathing-подключение с помощью NetApp ESX Host Utilities	35
5. Наилучшие решения IP-сети хранения	37
10 GB Ethernet	37
VLAN ID.....	37
Виртуальные интерфейсы NetApp	37
Использование коммутаторов Ethernet	38
Конфигурация для рабочей IP-инфраструктуры сети хранения.....	38
6. Варианты конфигурации сети VMware ESX	39

6.1 Создание высокодоступной IP-сети хранения с традиционными коммутаторами Ethernet	39
Введение в конфигурацию с несколькими портами VMkernel	39
Описание поведения адаптеров сервера ESX в случае отказа.....	39
Отказ коммутатора Ethernet.....	39
Масштабируемость сетевых соединений сервера ESX.....	40
6.2 ESX networking без EtherChannel	40
Преимущества.....	40
Недостаток	40
6.3 ESX с несколькими VMkernel, традиционным Ethernet, и NetApp с Single Mode VIFs.....	42
Преимущества.....	42
Недостатки	42
6.4 ESX с несколькими VMkernel, обычным Ethernet, и NetApp с Multi-Level VIFs	43
Преимущества.....	43
Недостатки	43
6.5 Конфигурация Datastore с традиционным Ethernet.....	44
6.6 IP-инфраструктура хранения высокой доступности с коммутаторами Ethernet Cross-stack EtherChannel	45
6.7 ESX Networking и Cross-stack EtherChannel	45
Преимущества.....	45
Недостатки	45
6.8 ESX, Cross-stack EtherChannel, и NetApp с Multimode VIFS	47
Преимущества.....	47
Недостаток	47
6.9 Конфигурация Datastore с использованием EtherChannel	47
7. Пути увеличения степени использования систем хранения	49
7.1 Дедупликация данных	49
Дедупликация с VMFS и RDM LUN	51
Дедупликация с NFS	52
7.2 Экономное распределение пространства (Thin Provisioning)	52
Опции Thin-Provisioning в NetApp	52
8. Управление и наблюдение	55
8.1 Наблюдение за системой хранения при помощи NetApp Operations Manager	55
8.2 Управление расширением объемов хранения.....	55
Расширение VMFS	55
Расширение виртуального диска (VMDK)	56
Расширение Raw Device Mapping (RDM)	57
Расширение файловой системы VM (NTFS или EXT3)	59
Расширение загрузочного тома с гостевой OS.....	59
9. Резервное копирование и восстановление	60
9.1 Технологии Snapshot	60
9.2 Размещение данных для Snapshot-копии	60
Размещение данных виртуальных машин	61
Registry file example script:	62
Размещение VMware Swap и Log File.....	62
10. Резервное копирование при помощи Snapshots в VMware	65
10.1 Использование NetApp Snapshot Backup для VMware Virtual Infrastructure.....	65
11. Выводы	66
12. ПРИЛОЖЕНИЕ 1: Конфигурирование системы для выполнения скрипта резервного копирования в Snapshot	67

12.1	Конфигурация ESX для использования Snapshot-копий	67
12.2	Конфигурирование SSH для использования с ESX Server и NetApp FAS	67
	Конфигурация системы хранения FAS для использования SSH	67
	Это пример ключа для хоста:	68
	Конфигурирование SSH для использования с ESX.....	68
	Пример вывода:.....	69
12.3	Восстановление Виртуальной Машины из Snapshot-копии VMFS.....	69
12.4	Восстановление Виртуальной Машины из Snapshot-копии NFS.....	70
12.5	Восстановление Виртуальной Машины из Snapshot-копии RDM	70
13.	ПРИЛОЖЕНИЕ 2: Пример Hot Backup Snapshot Script	72
14.	Ссылки	74
15.	История изменений.....	75

1. КРАТКО О ВАЖНОМ

Технологии NetApp позволяют компаниям расширить возможности их инфраструктуры, используя технологии виртуализированного хранилища данных NetApp для хранения данных их виртуальных серверов. NetApp предлагает решение, лидирующее в областях защиты данных; простоты распределения пространства хранения; экономного использования распределенного места; файлового резервного копирования; мгновенного резервного копирования и восстановления виртуальных машин (VM); моментального клонирования VM для целей тестирования, разработки приложений и обучения; создания простого и гибкого решения катастрофоустойчивости.

Данный документ рассматривает наилучшие методы решений при внедрении VMware Virtual Infrastructure, с использованием системы хранения Network Appliance FAS. Компания NetApp, в своих системах хранения, начала разработку опций для их использования в решениях VMware еще в 2001 году, когда этот продукт только появился на рынке. Все это время NetApp разрабатывал руководства для использования своих систем FAS с серверами ESX. Эти работы были задокументированы и проанализированы, с целью собрать вместе описание наилучших методов и данное руководство есть результат такой работы.

Тем не менее, описанная практика есть только рекомендация, но не требование. Невозможность следования описанным методикам не вызовет отказа в поддержке вашей системы компанией NetApp. Не все приведенные рекомендации применимы во всех возможных случаях. NetApp полагает, что пользователи найдут для себя полезным обдумать наши рекомендации, прежде чем приступят к выработке собственных практик, и принятию решений о внедрении подобной системы.

Аудитория этого документа предполагается знакомой с концепцией VMware ESX Server 3.5 и NetApp Data ONTAP® 7.X. Дополнительную информацию о преимуществах создания виртуальной инфраструктуры с использованием систем хранения NetApp можно посмотреть здесь: **NetApp and VMware ESX 3.0** <http://www.netapp.com/library/tr/3515.pdf>

Прим. переводчика:

Так как в настоящее время в русском языке нет устоявшихся и общепринятых терминов для многих понятий из текста оригинального документа, то при переводе использовались следующие термины (в скобках термины оригинального документа):

Сервер ESX (ESX Server) – хост-сервер виртуальных машин.

Датастор или datastore (также data store) – хранилище данных ESX, созданное на системе хранения

VMware cluster (ранее VMware data center) – группа серверов ESX объединенных в Virtual Infrastructure

ESX-нода (ESX node) – сервер ESX, входящий в VMware cluster

Агрегейт (aggregate) – логическое объединение физических дисков системы хранения

Том (volume) – основная базовая логическая единица разбивки пространства системы хранения

Экономное распределение (thin provisioning) – метод распределения ресурсов хранения

2. ВАРИАНТЫ ПОДКЛЮЧЕНИЯ СИСТЕМЫ ХРАНЕНИЯ К VMWARE

Существуют три способа подключения системы хранения к VMware Virtual Infrastructure 3 (VI3): VMFS Datastores, NAS Datastores, и raw device mappings (RDM). Данный раздел рассматривает эти варианты, и обобщает особенности для каждой архитектуры. Предполагается, что пользователь понимает, что общий массив хранения необходим для использования таких важных возможностей VMware, как HA, DRS, и VMotion™. Цель этого раздела дать пользователям информацию для планирования и разработки такой Virtual Infrastructure.

Заметьте: Нет необходимости при практическом внедрении выбирать только один из предложенных вариантов, напротив, VMware предлагает простые способы использовать любые из них параллельно и совместно.

2.1 VMFS DATASTORE ПОДКЛЮЧЕННЫЙ ПО FIBRE CHANNEL ИЛИ ISCSI

Virtual Machine File System (VMFS) Datastores это наиболее часто используемый метод использования хранилища в системе VMware. VMFS это кластерная файловая система, которая позволяет доступ к LUN-ам одновременно с разных серверов ESX, на каждом из которых запущено множество виртуальных машин. Преимущество этого решения в его высокой производительности, «взрослости» и отработанности технологии, а также легкости понимания принципов использования. Кроме этого VMFS предлагает администраторам VMware практическую независимость в своих действиях от группы администраторов системы хранения, так как когда хранилище выделено для использования с VMware, то администратор VMware свободен использовать пространство так, как ему необходимо, не взаимодействуя с администратором системы хранения. Большинство операций по управлению данными выполняются непосредственно через VMware VirtualCenter.

Проблема, связанная с такой схемой размещения данных состоит в трудностях анализа и оптимизации, наблюдения и масштабирования производительности ввода-вывода системы хранения. Так как датастор собирает в себе ввод-вывод множества виртуальных машин, то такая схема размещения не позволяет идентифицировать в общем потоке ввод-вывод отдельной виртуальной машины, хранящей свои данные на этом датасторе. На админа VMware ложится задача управления и наблюдения за нагрузкой ввода-вывода, которая ранее лежала на админе системы хранения. VMware VirtualCenter позволяет администраторам собирать и анализировать эти данные. NetApp представляет дополнительные данные по вводу-выводу, включая данные маппинга физической системы хранения виртуальным машинам, использование ресурсов ввода-вывода, и управления путями доступа с помощью VMInsight. VMInsight это часть продукта NetApp SANscreen®.

Для подробностей о доступе к виртуальным дискам, хранимым на VMFS с использованием FC или iSCSI, смотрите **VMware ESX Server 3.5 Configuration Guide**.

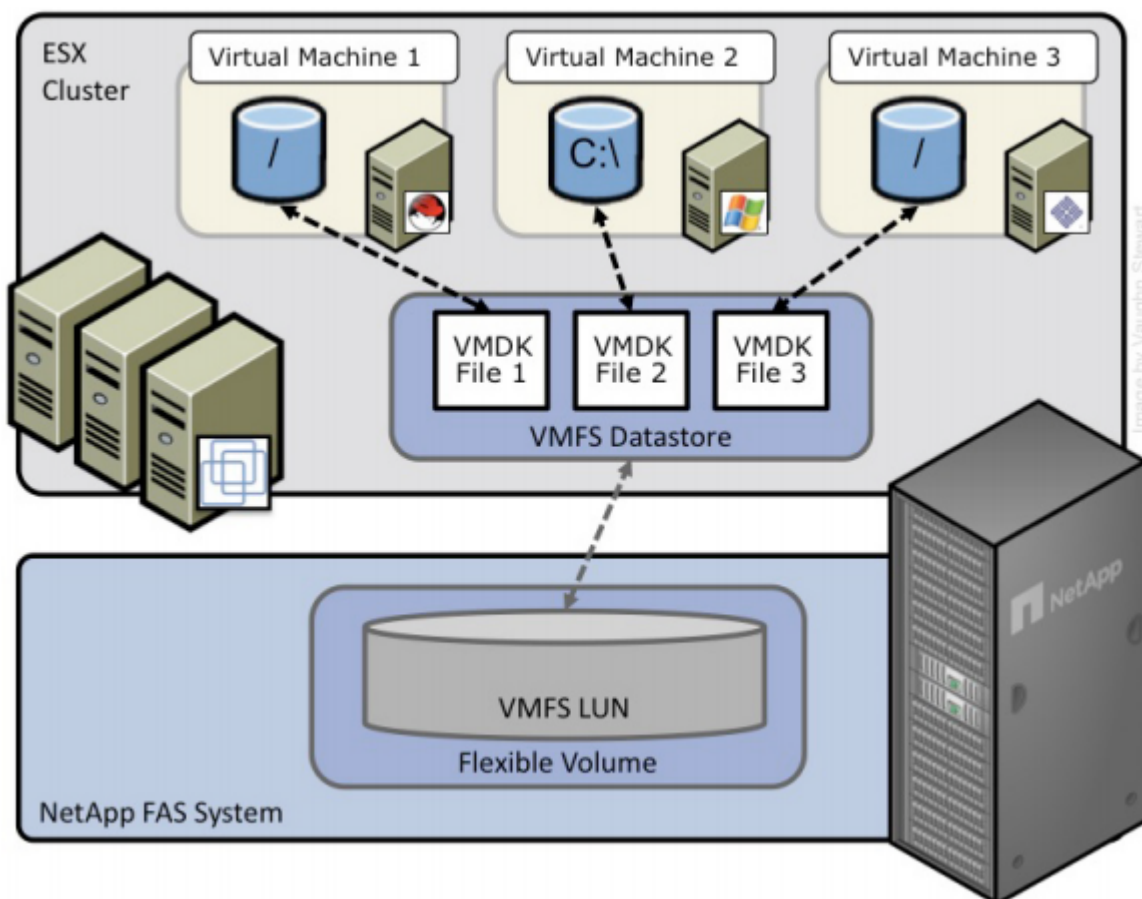


Рис. 1) ESX Cluster, подключенный к VMFS Datastore через FC или iSCSI.

2.2 NAS DATASTORE ПОДКЛЮЧЕННЫЙ ЧЕРЕЗ NFS

Хранение виртуальных дисков (VMDK) в сетевой файловой системе NFS появилось в VMware ESX 3.0. NFS Datastores набирает популярность как метод хранения в системе VMware. NFS позволяет одновременный доступ к томам от множества виртуальных машин на множестве серверов ESX. Преимущества данного решения сходны с преимуществами варианта с VMFS Datastores, когда один раз хранилище распределено для серверов ESX, то администратор VMware волен использовать его в соответствии со своими нуждами. Кроме этого преимуществами NFS Datastores является низкая цена «за порт» (в сравнении с Fibre Channel), высокая производительность, и экономичность за счет использования VMware thin provisioning, который используется по умолчанию для VMDK созданных на NFS.

Кроме опций самого датастора в VMware, NFS Datastores обеспечивает самый простой способ интеграции VMware со средствами управления и хранения данных в NetApp, таких как дедупликация, экономичное распределение (thin provisioning) на системе хранения, прямой доступ к нашим аппаратным снэпшотам (NetApp Snapshot™) и использование SnapRestore®.

Важнейшая проблема, связанная с развертыванием системы на NFS, связана с тем, что датастор на NFS пока не поддерживается в VMware Site Recovery Manager версии 1.0. Пользователям, использующим NFS, ищущим решение для обеспечения непрерывности бизнеса, приходится продолжать использовать ручное переключение при DR, пока не выйдет будущее обновление для Site Recovery Manager.

Рис. 2 показывает пример конфигурации. Обратите, что схема организации хранилища похожа на VMFS Datastore, однако каждый виртуальный диск имеет собственную очередь ввода-вывода (I/O queue), напрямую управляемую с системы NetApp FAS. Для подробностей о хранении файлов VMDK на NFS, смотрите **VMware ESX Server 3i Configuration Guide**

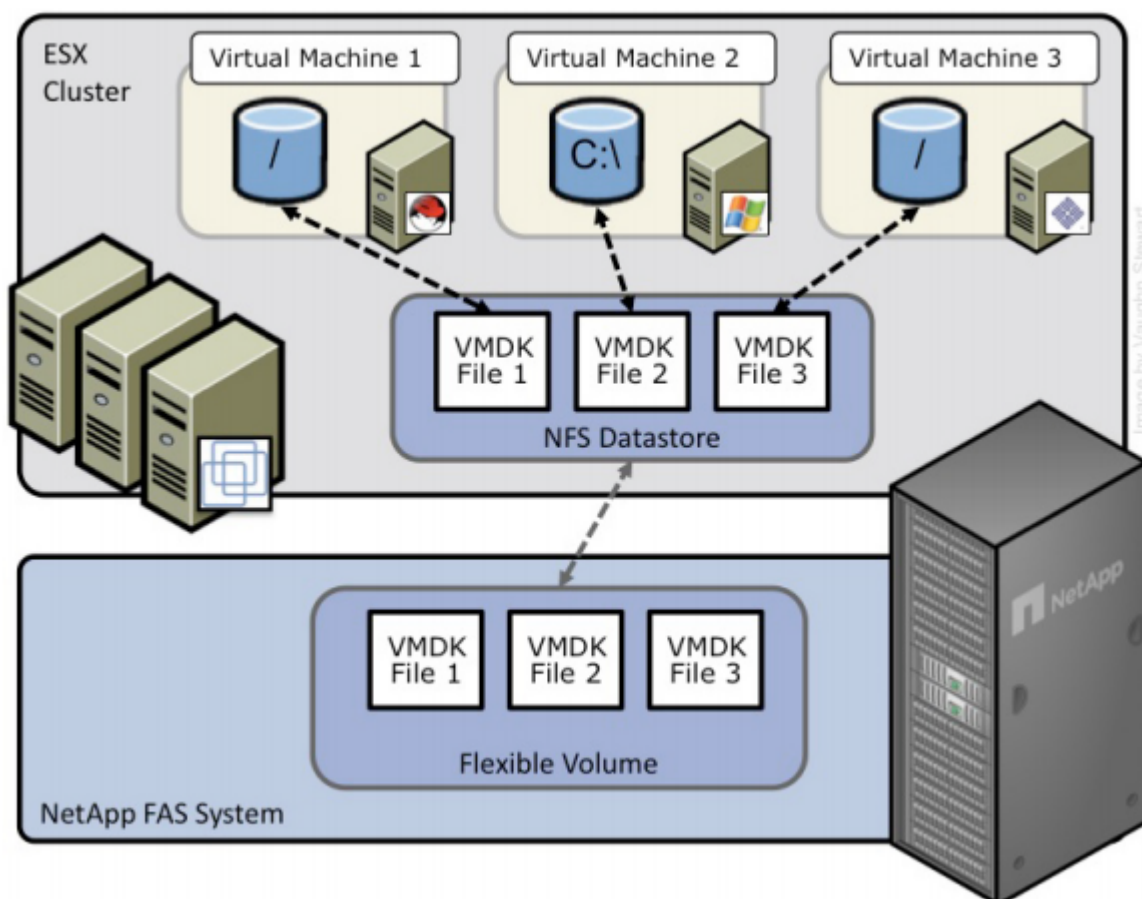


Рис. 2) ESX Cluster подключенный к NFS Datastore.

2.3 RAW DEVICE MAPPING ЧЕРЕЗ FIBRE CHANNEL ИЛИ ISCSI

Поддержка режима raw device mapping (RDM) появилась в VMware ESX Server 2.5. В отличие от VMFS и NFS Datastores, которые используют систему хранения как совместно используемый, глобальный пул, RDM предоставляет доступ к LUN непосредственно конкретной виртуальной машине. В этом случае, ESX действует как прокси между VM и системой хранения. Основное преимущество такого подхода это поддержка кластерных решений между виртуальными и между виртуальными и физическими машинами, такими как, например Microsoft® Cluster Server (MSCS). Кроме этого RDM обеспечивает высокий уровень производительности ввода-вывода, простоту измерения дисковой производительности на стороне дисковой системы, и простоту интеграции с такими возможностями, как SnapDrive®, гранулярные снапшоты VM, SnapRestore, и FlexClone®.

Проблемы такого решения заключаются в том, что кластер VMware оказывается ограничен в размерах, и такая схема требует для своей настройки взаимодействия между административными командами VMware и системы хранения. Рис. 3 показывает пример такой конфигурации. Обратите, что каждый виртуальный диск использует прямой ввод-вывод на выделенный LUN. Такая модель аналогична подключению физического сервера к SAN, исключая полосу пропускания канала контроллера, которая в этом случае используется совместно.

RDM доступен в двух режимах, физическом и виртуальном. Оба режима поддерживают основные функции VMware, такие как VMotion, и могут быть использованы как для HA, так и для DRS кластеров. Ключевое отличие между этими технологиями - степень виртуализации SCSI на уровне VM. Эти различия приводят к отдельным ограничениям в случаях использования MSCS и VMsnap. Для подробного рассмотрения raw device mappings по Fibre Channel и iSCSI, смотрите **VMware ESX Server 3i Configuration Guide**

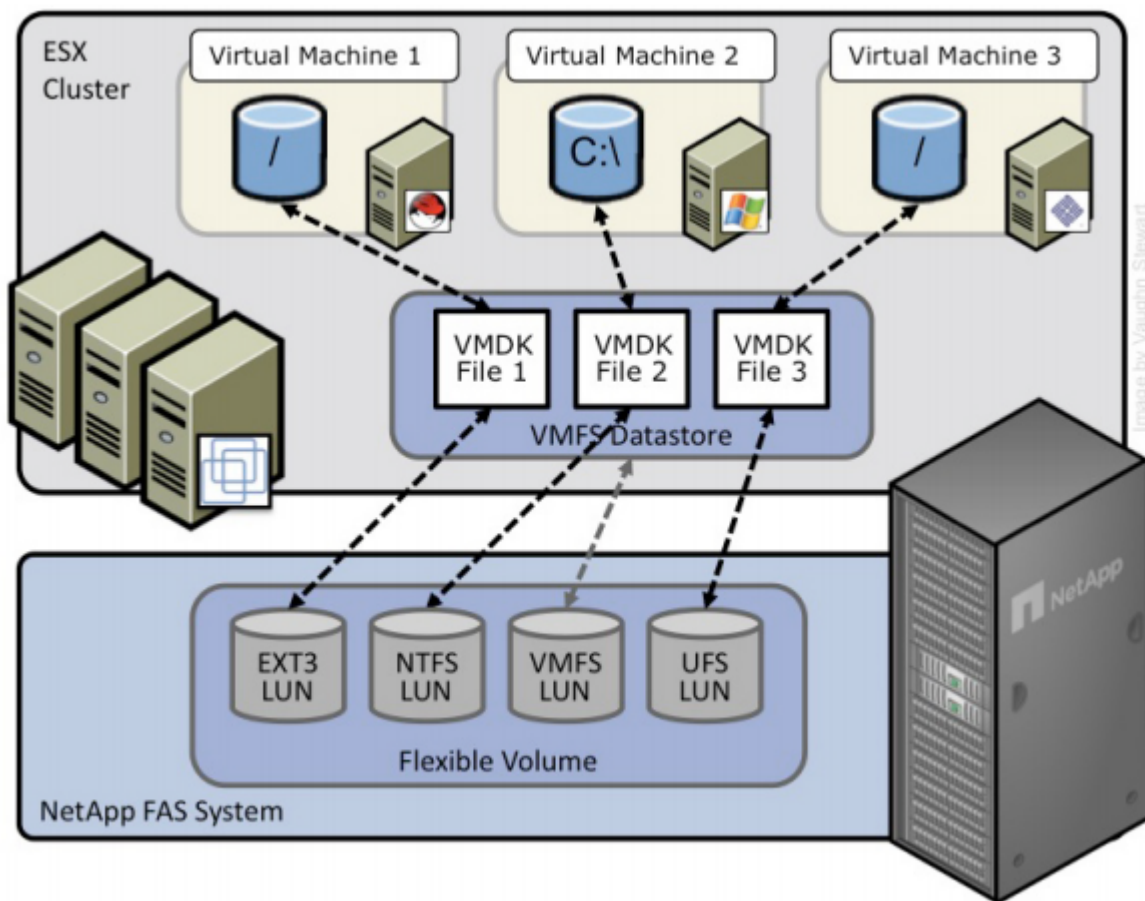


Рис. 3) ESX Cluster с VM, соединенными с RDM LUN-ами через FC или iSCSI.

2.4 ТАБЛИЦА СРАВНЕНИЯ МЕТОДОВ ДОСТУПА К DATASTORE

Таблица ниже сравнивает разные варианты подключения к datastore с использованием NetApp, и различные возможности доступные для каждого такого варианта. Похожая таблица также имеется в **VMware ESX Server 3i Configuration Guide**.

Возможности	FC	iSCSI	NFS
Format	VMFS или RDM	VMFS или RDM	NetApp WAFL®
Количество Datastores или LUNов	256	256	32
Размер Datastore	64TB	64TB	16TB
Количество VM на Datastore	32	32	N/A
Доступные скорости	1, 2, 4, 8 Gb/s	1, 10 Gb/s	1, 10 Gb/s
Варианты Backup			
VMDK image access	VCB	VCB	VCB, VIC File Explorer
VMDK file level access	VCB, только Windows®	VCB, только Windows®	VCB или 3rd party apps
NDMP granularity	LUN целиком	LUN целиком	Datastore, VMDK
Поддержка возможностей VMware			
VMotion	Да	Да	Да
Storage VMotion	Да	Да	Экспериментально
VMware HA	Да	Да	Да
DRS	Да	Да	Да
VCB	Да	Да	Да
MSCS support	Да, через RDM	Не поддерживается	Не поддерживается
Resize Datastore	Да, через extents Не рекомендуется в Production	Да, через extents Не рекомендуется в Production	Да, в production
Поддержка возможностей NetApp			
Snapshot copies	Да	Да	Да
SnapMirror®	Datastore или RDM	Datastore или RDM	Datastore или VM
SnapVault®	Datastore или RDM	Datastore или RDM	Datastore или VM
Data Deduplication	Да	Да	Да
Thin provisioning	Datastore или RDM	Datastore или RDM	Datastore
FlexClone	Datastore или RDM	Datastore или RDM	Datastore
Multistore	No	Да	Да
SANscreen	Да plus VMInsight	Да plus VMInsight	Да
Open Systems SnapVault	Да	Да	Да

Табл. 1) Сравнение различных методов доступа к Datastore.

3. КОНФИГУРИРОВАНИЕ И УСТАНОВКА NETAPP FAS

3.1 КОНФИГУРИРОВАНИЕ СИСТЕМЫ ХРАНЕНИЯ

Защита данных с помощью RAID

Существенным риском при консолидации является возможность сбоя платформы консолидации. Когда физический сервер превращен в виртуальный, и множество виртуальных машин помещено на физически одну платформу, влияние отказа этой платформы может быть катастрофическим. К счастью VMware обеспечивает множество технологий высокой доступности, расширяющей возможности виртуальной инфраструктуры. Сюда входят кластеризация физических серверов через VMware HA, балансировки нагрузки с помощью DRS, и возможности непрерывающей работу перемещения виртуальных машин и их данных между физическими серверами ESX с помощью VMotion и Storage VMotion соответственно.

Когда во главу угла ставится доступность данных, то возможно много разных вариантов создания отказоустойчивого решения, куда входят приобретение физических серверов с резервными интерфейсами и HBA, развертывание избыточных средств сетевой инфраструктуры и сетевых путей, а также использование систем хранения с избыточными контроллерами. Системы хранения должны обеспечивать удовлетворение требования отсутствия единой точки отказа.

На практике, требования защиты данных для виртуальных инфраструктур выше, чем для традиционной инфраструктуры физических серверов. Защита данных стоит во главе угла для совместно используемого устройства хранения. NetApp RAID-DP® это улучшенная технология RAID, предлагаемая как уровень RAID по умолчанию для всех систем хранения FAS. RAID-DP защищает от одновременной потери двух дисков в одной RAID-группе. Использование RAID-DP весьма экономично, так как оверхед по дисковой емкости составляет всего 12,5% при размере RAID-группы по умолчанию. Этот уровень надежности и эффективности хранения делает размещение данных на RAID-DP более безопасным чем на RAID 5 и более экономным, чем на RAID 10. NetApp рекомендует использовать RAID-DP для всех RAID-групп, которые хранят данные VMware.

Aggregates

«Агрегейт» (aggregate) это «виртуализационный слой» NetApp, который абстрагирует логические тома, так называемые *flexible volumes* от физических дисков. Создание тома поверх агрегейта означает, что ввод-вывод для этого тома будет использовать возможности всех входящих в его пул физических дисков, что повышает показатели IOPS. Такое решение хорошо подходит в случае слабопредсказуемых и смешанных нагрузок по вводу-выводу. NetApp рекомендует, когда это возможно, создавать отдельный маленький aggregate для root-раздела. Этот aggregate будет хранить файлы, требуемые для управления системой хранения и ее служебные файлы. Оставшееся пространство хранения рекомендуется помещать в минимальное количество больших aggregates. Общий характер ввода-вывода от VMware традиционно предельно случаен по своей природе, поэтому такая модель распределения дисков обеспечивает оптимальную производительность, так как операции ввода-вывода распределяются равномерно по большому числу «шпинделей» физических жестких дисков. На маленьких системах, с малым числом дисков, может быть несколько непрактичным отделять диски в маленький aggregate, в таком случае вполне приемлемо делать единый общий aggregate на всю систему хранения.

Flexible Volumes (FlexVol)

Тома типа Flexible хранят LUN-ы, или непосредственно файлы виртуальных дисков, к которым обращается сервер VMware ESX. NetApp рекомендует заводить по одному VMware

Datastore на соответствующий flexible volume. Такой дизайн позволяет легко разобраться и понять структуру хранения данных в VMware, когда вы смотрите на конфигурацию системы хранения данных. Такая модель соответствия также упрощает использование резервных копий при помощи Snapshot, разработку политик репликаций SnapMirror на уровне Datastore, так как NetApp реализовывает эту функциональность именно на уровне flexible volume.

LUN

LUN-ы это логические устройства, созданные на системе хранения FAS, и непосредственно подключенные к серверу ESX. Сервер ESX может быть соединен с LUN-ами двумя способами. Первый и наиболее распространенный метод – как хранилище виртуальных дисков для множества виртуальных машин. Этот тип использования принято называть Virtual Machine File System (VMFS) LUN. Второй метод это так называемый «Raw Device Mapping» (RDM). При RDM, LUN подключен к ESX Server и передается непосредственно виртуальной машине для создания на нем ее собственной (native) файловой системы, например NTFS или EXT3.

Для подробного рассмотрения темы обратитесь к **VMware Storage/SAN for ESX Server 3.5 and ESX Server 3i**.

Соглашение о порядке именовании

Системы хранения NetApp позволяют использовать «человекочитаемые» имена при создании элементов хранения. Хорошо спроектированная виртуальная инфраструктура использует самоописывающиеся имена, которые помогают идентифицировать и правильно соединять системы хранения и виртуальные машины. Простое и продуманное правило именования также упрощает конфигурирование репликации и процессов восстановления после сбоев.

Воспользуйтесь следующими рекомендациями:

- **Имя тома:** Должно соответствовать имени «датацентра» или имени «датацентра» и политике репликации или же типу хранимых данных (например, **Datastore1**, **Datastore1_4hr_Mirror**)
- **Имя LUN:** для VMFS, NetApp рекомендует давать имя, соответствующее имени datastore.
- **Имя LUN:** для RDM, рекомендует создавать имя с использованием имени хоста и имени тома конкретной виртуальной машины (например, для Windows®, **hostname_c_drive.lun**, для Linux VM **hostname_root.lun**, и т.д.)

4. ОСНОВЫ КОНФИГУРИРОВАНИЯ VIRTUAL INFRASTRUCTURE 3

4.1 ОГРАНИЧЕНИЯ И РЕКОМЕНДАЦИИ КОНФИГУРИРОВАНИЯ

При создании хранилища вы должны учитывать следующие ограничения и рекомендации.

Опции томов NetApp

Тома NetApp должны создаваться как flexible volumes, с параметром snap reserve установленным в 0 и отключенным расписанием создания снэпшотов. Все Snapshot-копии системы хранения NetApp должны быть скоординированы с серверами ESX, чтобы быть уверенным в обеспечении целостности и непротиворечивости сохраняемых данных. Тема Snapshot-копий NetApp рассмотрена ниже в главе **10.1 Использование Snapshot-копий**. Для установки опций тома на рекомендованные значения, выполните следующие действия в системной консоли FAS.

1. Войдите в консоль NetApp.
2. Установите volume Snapshot schedule:
`snap sched <vol-name> 0 0 0`
3. Установите volume Snapshot reserve:
`snap reserve <vol-name> 0`

RDM и ограничения на размер в VMware Cluster

В настоящее время размер VMware cluster ограничен общим числом в 256 LUN-ов на ESX-сервер. Это ограничение обычно существенно только в инсталляциях, использующих RDM как основную форму хранилища виртуальных машин. Используя RDM, вы должны запланировать дополнительно пару VFMS LUN-ов для хранения конфигурационных файлов

Отметьте, что VMDK definition file, связанный с RDM LUN показывается размером равным размеру соответствующего ему LUN. Это нормальное поведение для VirtualCenter; реальный размер VMDK definition file, который будет занят на диске, составляет несколько мегабайт (обычно между 1 и 8 мегабайтами, размером блока в VMFS).

Для определения числа узлов ESX на VMware Cluster, вы можете воспользоваться формулой:

$254 / (\text{планируемое число VMs на ESX хост}) / (\text{кол-во RDMS на VM}) = \text{число ESX узлов в датацентре}$

Отметьте, что эта формула применима к тем случаям, когда все узлы в кластере соединены со всеми разделяемыми LUN

Например, если вы собираетесь запустить 20 VM на ESX Server и хотите подключить по 2 RDM на виртуальную машину (VM), то формула будет:

$254/20/2 = 6.4$ округляем вверх = 7 ESX узлов в датацентре

Правила создания LUN для VMFS Datastores

VMFS Datastore предлагает самый простой метод создания и распределения пространства хранилища; однако необходимо соблюдать баланс между множеством datastores и одним, но перегруженным множеством находящихся в нем VM. В последнем случае следует выравнять нагрузку по вводу-выводу. VMware обеспечивает функцию Storage VMotion что означает возможность перемещать хранилище VM на другие Datastores без прерывания работы самой VM. Обычно большие VMFS Datastores достигают предела по вводу-выводу раньше, чем предела по объему. Новые технологии распределения пространства, такие как «thin provisioning» могут помочь вернуть распределенное, но неиспользуемое пространство

хранения в пул свободного места на FAS, с тем, чтобы можно было использовать его для более нуждающихся в нем задачах.

Неиспользуемое пространство хранения не включается в процесс удаления или миграции при Storage VMotion. Несмотря на то, что нет определенных рекомендаций относительно размеров VMFS Datastore, его принято делать в пределах от 300 до 700GB. Максимальный поддерживаемый размер LUN равен 2TB. Для подробностей смотрите документ VMware Storage/SAN Compatibility Guide for ESX Server 3.5 and ESX Server 3i.

Ограничения для NFS Datastore

По умолчанию, VMware ESX позволяет иметь 8 NFS datastor-ов; это ограничение может быть расширено до 32. Для больших систем NetApp рекомендует увеличивать это значение до максимума.

Чтобы сделать это, проделайте следующие шаги в Virtual Infrastructure client. Для подробностей смотри: **KB2239 NFS Mounts are Restricted to 8 by Default** в Knowledge Base на сайте VMware.

1. Откройте VirtualCenter.
2. Выберите хост ESX.
3. В правой панели выберите закладку Configuration.
4. В поле Software, выберите Advanced Configuration.
5. В появившемся окне, выберите NFS в левой панели.
6. Измените величину NFS.MaxVolumes на 32. См. рис. 4.
7. В появившемся окне выберите Net в левой панели.
8. Измените величину Net.TcpIpHeapSize на 30.
9. Измените величину Net.TcpIpHeapMax на 120
10. Повторите для каждого сервера ESX.

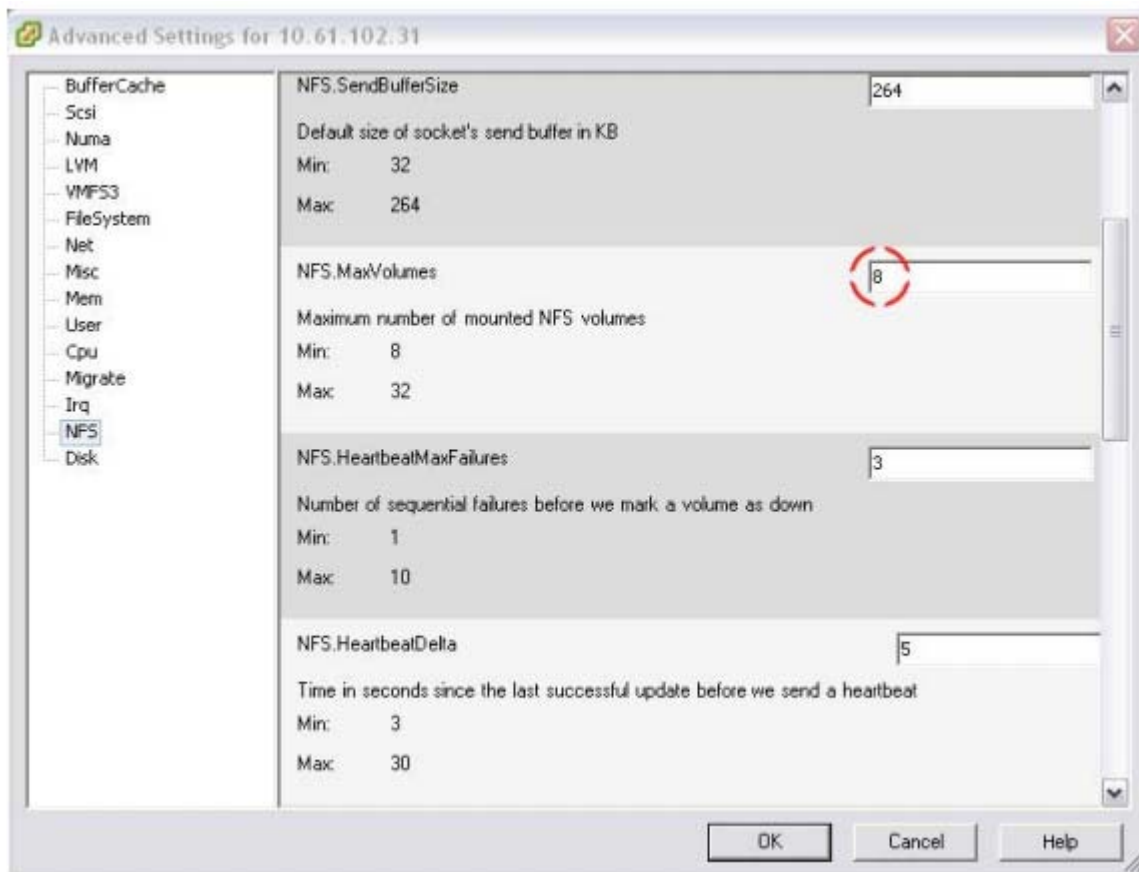


Рис. 4) Увеличение числа NFS Datastores.

Дополнительные рекомендации по NFS

Когда вы устанавливаете VMDK на NFS, то сделайте следующие изменения в настройках, для достижения наилучшей производительности.

- 1 Войдите в консоль NetApp.
- 2 Введите команду
`vol options <vol-name> no_atime_update on`
- 3 Повторите шаг 2 для каждого тома NFS.
- 4 В консоли введите команду
`options nfs.tcp.recvwindowsize 64240`

VMware ESX Server имеет собственный механизм создания снэпшотов. Процесс удаления снэпшота VMware (или проведения (commit) файлов VMsnap log) может вызывать проблему, когда ввод-вывод гостевой OS зависает на продолжительное время если Datastores подключены по NFS.

Снэпшоты VMware используются для виртуальных машин на NFS Datastores. Это использование включает себя, но не ограничивается только: VMware Snapshots, Storage VMotion, Consolidated Backup, NetApp SnapManager for Virtual Infrastructure, и так далее.

Такое поведение описано VMware в SR195302591. Эта проблема была решена в ESX 3.5 update 3; однако некоторые дополнительные шаги должны быть выполнены для применения этого исправления. Выпущенный патч выпущен для систем ESX 3.5 update 1 или update 2. Внимание: Когда используется патч ESX350-200808401-BG, возможны случаи, когда виртуальная машина неожиданно может перейти в powered off.

Эти случаи:

1. Посторонние клиенты (3rd party), такие как агенты управления виртуальными машинами, использующие 'read-only' локирование файлов виртуального диска, во время процесса VMware snapshot commit.

2. Ручное создание снимка виртуальной машины пользователем, в то время, когда происходит процесс commit существующего снимка VMware.

Чтобы избежать таких проблем, выключите сторонние клиенты во время процесса commit снимка VMware.

Применение патчей к системе под ESX и ESXi 3.5 update 3:

- 1 С помощью VMotion перенесите запущенные виртуальные машины на другую ноду ESX
- 2 Переведите сервер ESX в maintenance mode
- 3 Убедитесь, что в advanced configuration option для NFS locks стоит 0
- 4 Сохраните файл /etc/vmware/config
- 5 Вставьте в файл /etc/vmware/config следующую строку
prefvmx.consolidateDeleteNFSLocks = "TRUE"
- 6 Перезагрузите сервер ESX
- 7 После завершения перезагрузки залогиньтесь и выйдите из maintenance mode
- 8 Переместите ваши VM назад, на патченный сервер ESX и проверьте создание lock-файла в корневой директории этой VM. Lock-файл имеет расширение .lck
- 9 Если lock-файл создается, повторите шаги от 1 до 7 на каждом сервере ESX
- 10 Если lock-файл не создается, то убедитесь, что вы следовали всем шагам в точности. Если lock-файл по-прежнему не создается, то возможно необходимо рестартовать VM.

Следующая подгруппа команд поможет автоматизировать изменения перечисленные выше. Она требует входа на сервер ESX через CLI. Это заменяет шаги от 2 до 6 в перечисленном выше процессе. Приведенные 5 строк должны быть исполнены из консоли ESX под root.

1. vimsh -n -e /hostsvc/maintenance_mode_enter
2. esxcfg-advcfg -s 0 /NFS/LockDisable
3. cp -p /etc/vmware/config /etc/vmware/config.bak
4. echo prefvmx.consolidateDeleteNFSLocks = "TRUE" >>
/etc/vmware/config
5. reboot

После этого выполните все действия от 7 до 10 вышеприведенного процесса патчения ESX 3.5 update 3.

Применение патчей к системе под ESX и ESXi 3.5 update 1 или update 2:

1. Скачайте патч **ESX350-200808401-BG**
2. Определите сервера, которые требуют установки этого патча и проверьте все необходимые условия его установки
3. Установите патч
4. С помощью VMotion перенесите запущенные виртуальные машины на другую ноду ESX

5. Переведите сервер ESX в maintenance mode
6. Убедитесь, что в advanced configuration option для NFS locks стоит 0
7. Сохраните файл /etc/vmware/config
8. Вставьте в файл /etc/vmware/config следующую строку
prefvmx.consolidateDeleteNFSLocks = "TRUE"
9. Перезагрузите сервер ESX
10. После завершения перезагрузки залогиньтесь и выйдите из maintenance mode
11. Переместите ваши VM назад, на патченный сервер ESX и проверьте создание lock-файла в корневой директории этой VM. Lock-файл имеет расширение .lck
12. Если lock-файл создается, повторите шаги от 2 до 10 на каждом сервере ESX
13. Если lock-файл не создается, то убедитесь, что вы следовали всем шагам в точности. Если lock-файл по-прежнему не создается, то возможно необходимо рестартовать VM.

Следующая подгруппа команд поможет автоматизировать изменения перечисленные выше. Она требует входа на сервер ESX через CLI. Это заменяет шаги от 5 до 9 в перечисленном выше процессе. Приведенные 5 строк должны быть исполнены из консоли ESX под root.

1. vimsh -n -e /hostsvc/maintenance_mode_enter
2. esxcfg-advcfg -s 0 /NFS/LockDisable
3. cp -p /etc/vmware/config /etc/vmware/config.bak
4. echo prefvmx.consolidateDeleteNFSLocks = "TRUE" >>
/etc/vmware/config
5. reboot

После этих действий выполните шаги с 10 по 13 из процесса патчения систем ESX 3.5 update 1 и 2.

О системах под ESX или ESXi версий до 3.5 update 1:

Если вы используете скрипты для создания дисковых снэпшотов для резервного копирования, и не имеете возможности обновить систему, то VMware и NetApp рекомендуют не пользоваться процессом VMsnap до создания снэпшота NetApp.

Начальное смещение Виртуального Диска

Виртуальные машины хранят свои данные на виртуальных дисках, и эти диски сформатированы в ту или иную файловую систему, которая позволяет виртуальной машине хранить на них данные. Когда вы форматируете виртуальный диск, важно убедиться, что файловая система VMDK, datastore, и раздел самой системы хранения правильно выровнены между собой. Ошибка в выравнивании файловой системы обычно вызывает снижение производительности. Однако даже если файловая система выровнена неоптимально, снижение производительности может и не быть заметно, например если система хранения имеет достаточный запас производительности. Тем не менее, любой производитель систем хранения, так или иначе, сталкивается с этой проблемой. Для подробностей смотрите публикацию VMware: **Recommendations for Aligning VMFS Partitions**.

Для того чтобы выровнять партицию виртуального диска при использовании системы хранения NetApp FAS, начальное смещение должно делиться нацело на 4096. Рекомендованная величина стартового смещения – 32768. Значение по умолчанию в Windows 2008 & Vista равно 1048576 и не удовлетворяет этим условиям. Для OS Windows в качестве «гостевой системы» виртуальной машины, проверить эту величину достаточно

просто. Запустите утилиту msinfo32, и скорее всего вы найдете, что VM работает с начальным смещением по умолчанию в 32256. См. рис. 5.

Msinfo32 может быть запущен выбором:

Start > All Programs > Accessories > System Tools > System Information.

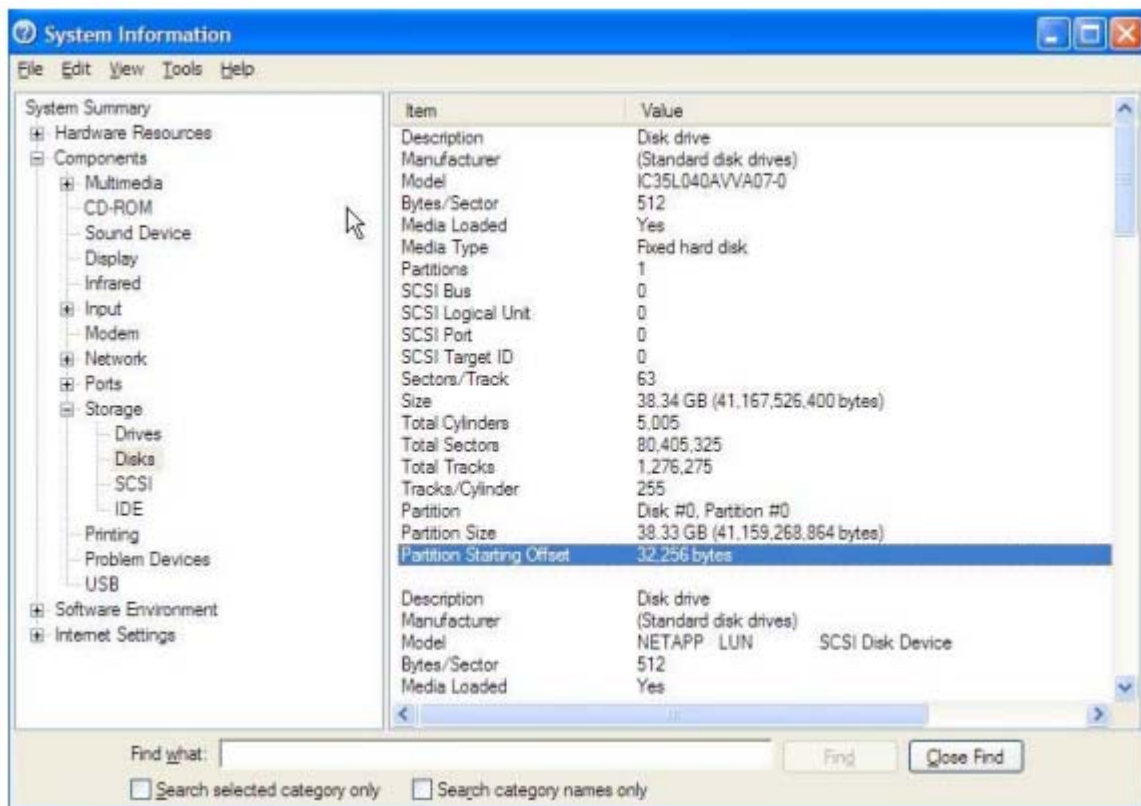


Рис. 5) Использование приложения system information для определения смещения партии.

Исправить начальное смещение лучше всего в шаблоне, из которого вы в дальнейшем будете создавать новые виртуальные машины.

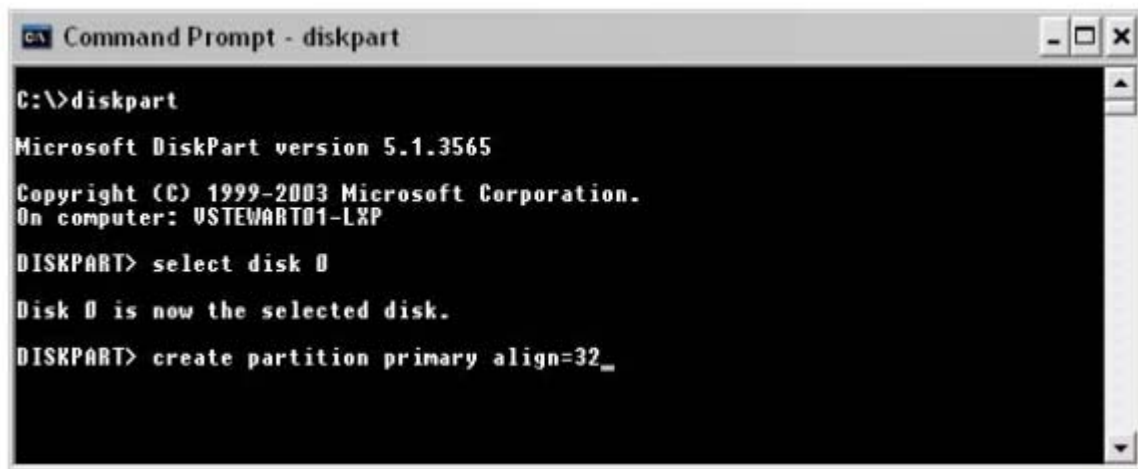
Для уже установленной и работающей с неверным смещением виртуальной машины, NetApp рекомендует исправлять смещение, только если VM испытывает проблемы с производительностью ввода-вывода. Влияние на производительность может быть более заметно для систем, производящих много операций чтения-записи мелкими блоками. Для того чтобы выровнять смещение партии виртуальной машины, вам надо создать новый виртуальный диск, после чего мигрировать данные виртуальной машины с исходного диска на новый. Невыровненная виртуальная машина, но с малым количеством операций ввода-вывода не получит от проведения такого выравнивания каких-то заметных преимуществ.

Форматирование с правильным Partition Offsets

Виртуальные диски могут быть сформатированы с правильным offset в момент создания, если мы загрузим виртуальную машину до установки OS и вручную зададим желаемый offset. Для OS Windows в качестве «гостевой системы» виртуальной машины, имеется отличный инструмент Windows Preinstall Environment boot CD. Для установки partition offset, выполните следующие шаги и смотрите рис. 6.

1. Загрузите VM при помощи WinPE CD.
2. Выберите Start > Run и введите Diskpart.
3. Введите Select Disk0.
4. Введите Create Partition Primary Align=32.

5. Перезагрузите VM.
6. Установите операционную систему обычным образом.



```
C:\>diskpart
Microsoft DiskPart version 5.1.3565
Copyright (C) 1999-2003 Microsoft Corporation.
On computer: USTEWART01-LXP

DISKPART> select disk 0
Disk 0 is now the selected disk.
DISKPART> create partition primary align=32_
```

Рис. 6) Запуск diskpart для установки правильного смещения партии.

Оптимизация файловой системы Windows для наилучшей производительности ввода-вывода

Если ваша виртуальная машина не работает как файловый сервер, то вы можете применить следующие параметры, чтобы запретить изменения атрибута access time в NTFS. Это изменение снизит количество операций ввода-вывода, производимых файловой системой. Чтобы сделать эти изменения следуйте шагам:

1. Залогиньтесь в виртуальную машину Windows
2. Выберите Start > Run и введите cmd
3. Введите fsutil behavior set disablelastaccess 1

4.2 РАСПРЕДЕЛЕНИЕ ПРОСТРАНСТВА ХРАНЕНИЯ

С выходом VMware Virtual Infrastructure 3.0, появилось и несколько новых опций в области использования систем хранения данных. Этот раздел рассматривает вопросы распределения пространства системы хранения при использовании Fibre Channel, iSCSI, и Network File System (NFS).

Требования VMware для Fibre Channel и iSCSI

VMware обнаружила ошибку, которая влияет на стабильность соединений с хостами по FCP и iSCSI, и выпустила патч ESX350-200808402-BG, который исправляет эту ошибку. В настоящий момент, этот патч применяется только к ESX version 3.5, updates 1 и 2.

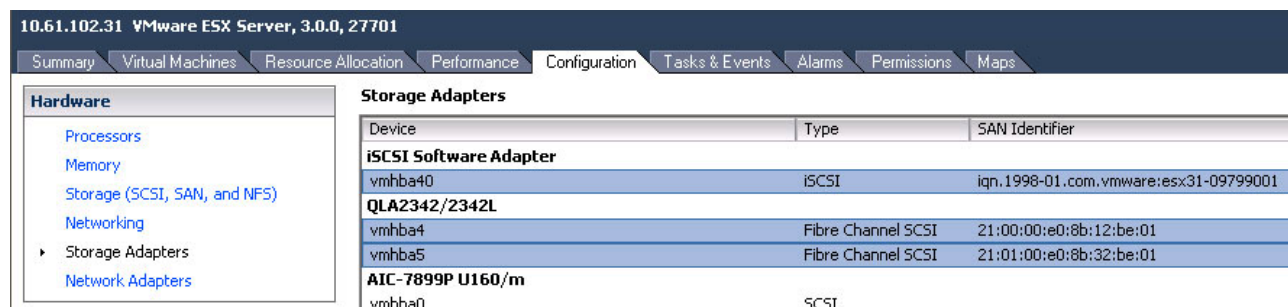
Распределение пространства хранения на Fibre Channel и iSCSI LUN

Для создания LUN с доступом через FCP или iSCSI, сначала нужно создать initiator group (igroup) на системе хранения FAS. В NetApp igroup являются видом LUN masking, регулирующим доступ хоста к LUN. NetApp рекомендует создавать igroup для каждого VMware cluster. Дополнительно, NetApp предлагает включать имя igroup имя VMware cluster и тип протокола (например, DTW_DC1_FCP и DTW_DC1_i SCSI).

Эта схема именования и метод упрощения управления igroup-ами уменьшает общее их число. Это также обеспечивает то, что все сервера ESX входящие в cluster видят каждый LUN под теми же ID. Каждая initiator group включает в себя все FCP worldwide port names (WWPN) или iSCSI qualified names (IQN) каждого сервера ESX в VMware datacenter.

Внимание: Если VMware cluster использует и Fibre Channel и iSCSI, создавайте отдельные igroups для Fibre Channel и iSCSI.

Чтобы найти WWPN или IQN для конкретного сервера ESX, выберите storage adapter в закладке Configuration соответствующего сервера ESX в VirtualCenter и посмотрите его в колонке SAN Identifier. См. рис. 7.



The screenshot shows the VMware ESX Server configuration interface. The top navigation bar includes tabs for Summary, Virtual Machines, Resource Allocation, Performance, Configuration, Tasks & Events, Alarms, Permissions, and Maps. The left sidebar shows a tree view under 'Hardware' with options for Processors, Memory, Storage (SCSI, SAN, and NFS), Networking, Storage Adapters (selected), and Network Adapters. The main content area displays a table of Storage Adapters.

Device	Type	SAN Identifier
iSCSI Software Adapter		
vmhba40	iSCSI	iqn.1998-01.com.vmware:esx31-09799001
QLA2342/2342L		
vmhba4	Fibre Channel SCSI	21:00:00:e0:8b:12:be:01
vmhba5	Fibre Channel SCSI	21:01:00:e0:8b:32:be:01
AIC-7899P U160/m		
vmhba0	SCSI	

Рис. 7) Определение WWPN и IQN в Virtual Infrastructure client.

LUN-ы могут быть созданы при помощи NetApp LUN wizard в системной консоли FAS или при помощи FilerView® GUI.

Следующие процедуры показывают процесс создания LUN при помощи FilerView GUI.

1. Войдите в FilerView.
2. Выберите LUN.
3. Запустите Wizard.
4. В окне Wizard, нажмите Next.
5. Введите путь. См. рис. 8.
6. Введите размер LUN.
7. Введите тип LUN (для VMFS выберите VMware; для RDM выберите тип как у VM).
8. Введите описание и нажмите Next.

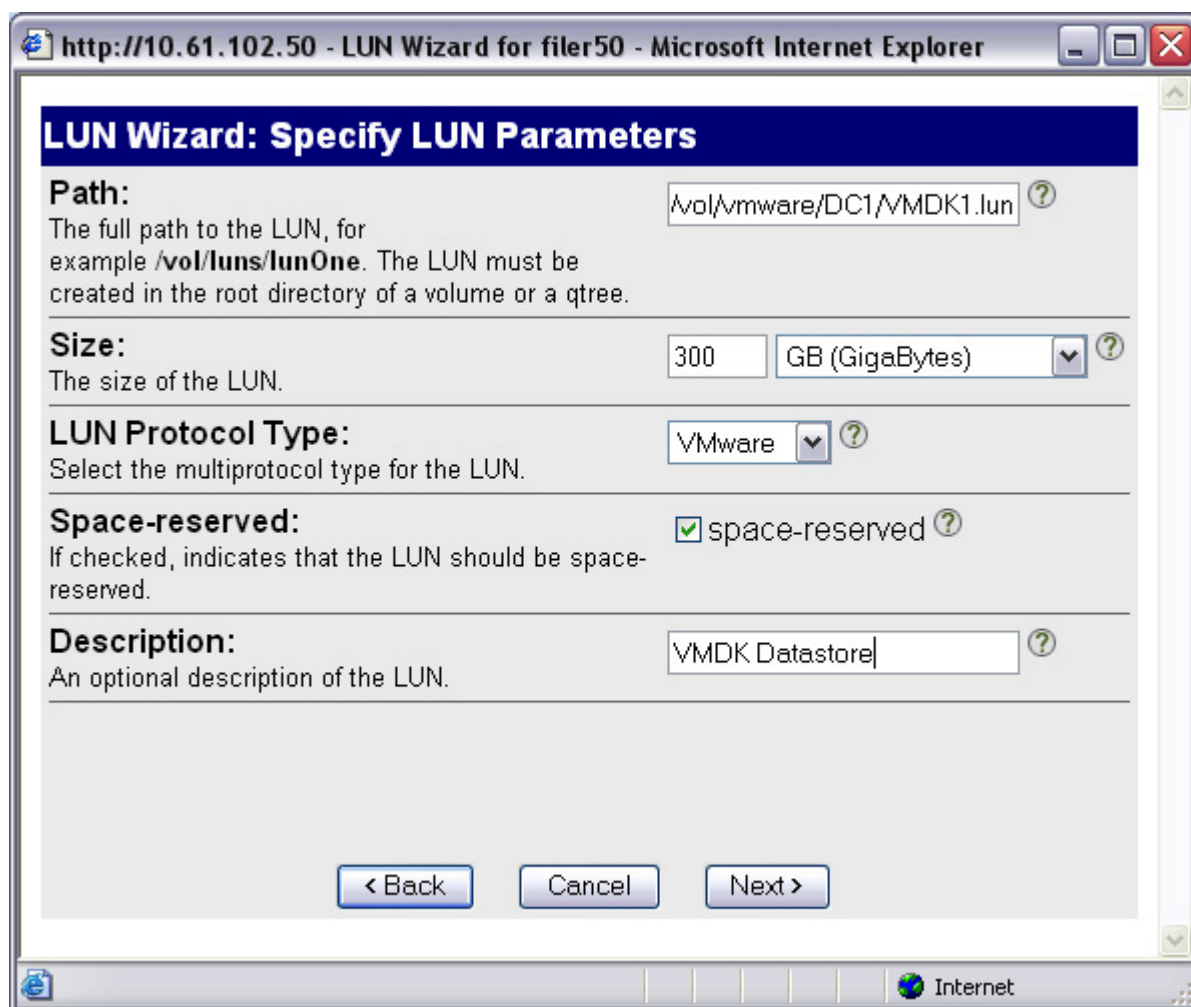


Рис. 8) NetApp LUN Wizard.

Следующий шаг в LUN wizard это LUN masking. LUN masking позволяет сопоставить необходимую igroup соответствующему LUN.

В LUN wizard, вы можете, как назначит уже существующую igroup, так и создать новую igroup.

Важно: Сервер ESX ожидает, что LUN ID будет один и тот же на каждой ноде в ESX cluster. Поэтому NetApp рекомендует создавать одну igroup для каждого кластера, вместо одной на каждый ESX Server.

Для конфигурирования LUN masking для LUN, создаваемого в FilerView GUI, проделайте следующие шаги.

1. Выберите Add Group.
2. Выберите радиокнопкой Use Existing Initiator Group. Нажмите Next и продолжайте шагом 3а.
или
Выберите радиокнопкой Create a New Initiator Group. Нажмите Next и продолжайте шагом 3б.
- 3а Выберите группу из списка, и назначьте LUN ID или оставьте поле пустым (система сама назначит подходящий). Нажмите Next для завершения.
- 3б Для создания новой группы, введите необходимые параметры для igroup, такие как имя, тип соединения (FCP или iSCSI), и тип OS (VMware), и нажмите Next. См. рис. 9.
4. Введите новый или выберите существующий SAN Identifiers (WWPN или IQN) для системы, к которой будет подключен LUN.

5. Нажмите кнопку Add Initiator.
6. Нажмите Next для завершения процедуры.

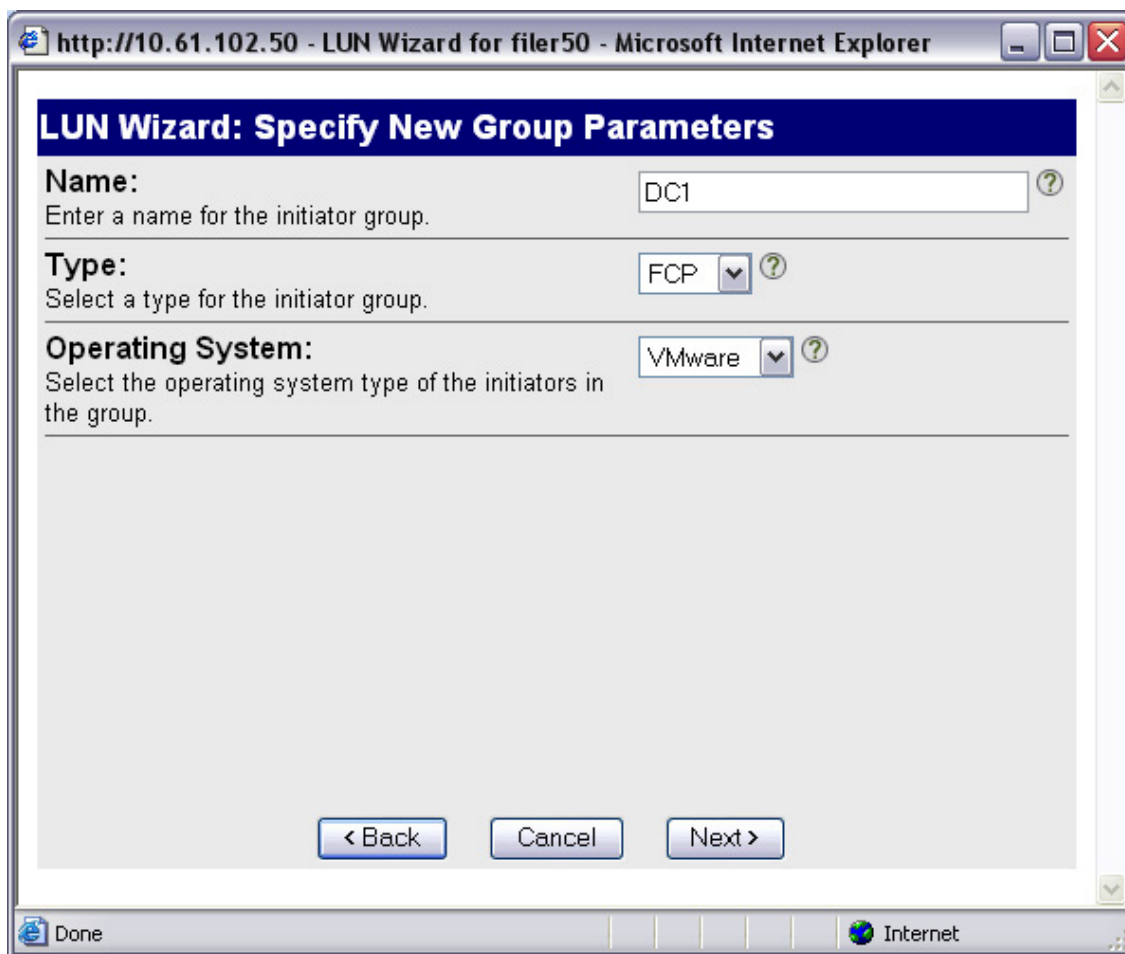


Рис.9) Назначение igroup для LUN.

4.3 РАСПРЕДЕЛЕНИЕ ПРОСТРАНСТВА ХРАНЕНИЯ НА NFS

Если вы предпочли использовать виртуальные диски на NFS, то процесс прост. При создании файловой системы для использования ее как NFS datastore, проделайте следующие шаги.

1. Откройте FilerView (http://filer/na_admin).
2. Выберите Volumes.
3. Выберите Add, чтобы открыть Volume Wizard. См. рис. 10. Выполните Wizard.
4. Из меню FilerView, выберите NFS.
5. Выберите Add Export, чтобы открыть NFS Export Wizard. См. рис. 11. Выполните Wizard для создания новой файловой системы, предоставив права **read/write** и **root access** для адресов VMkernel всех хостов ESX, которые будут подключаться к экспортируемой файловой системе.
6. Откройте VirtualCenter.
7. Выберите хост ESX.
8. В правой панели выберите закладку Configuration.
9. В поле Hardware щелкните Storage.
10. В верхнем правом углу, щелкните Add Storage чтобы открыть Add Storage Wizard. См. рис. 12.

11. Выберите радиокнопку Network File System и нажмите Next.
12. Введите имя системы хранения, export, и datastore, и нажмите Next. См. рис. 13
13. Нажмите Finish.

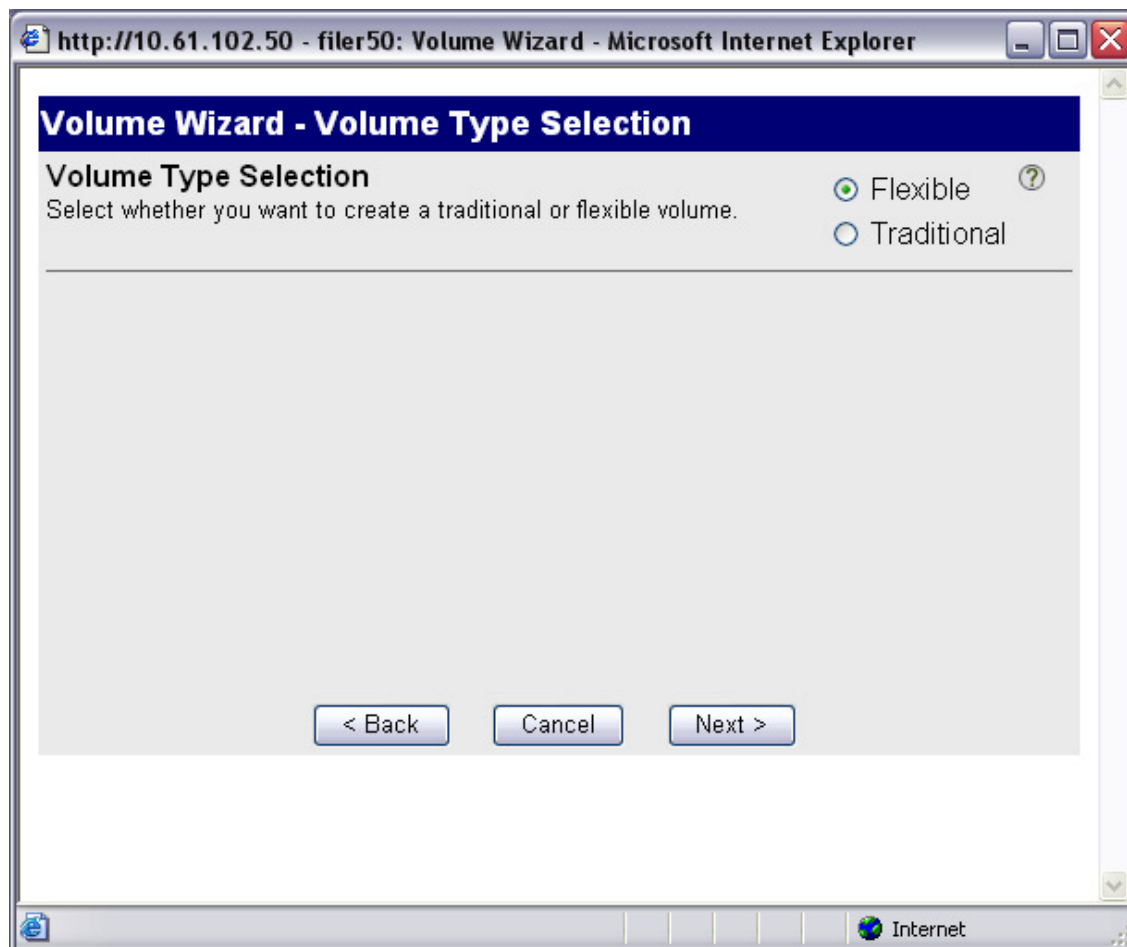


Рис. 10) NetApp Volume Wizard.

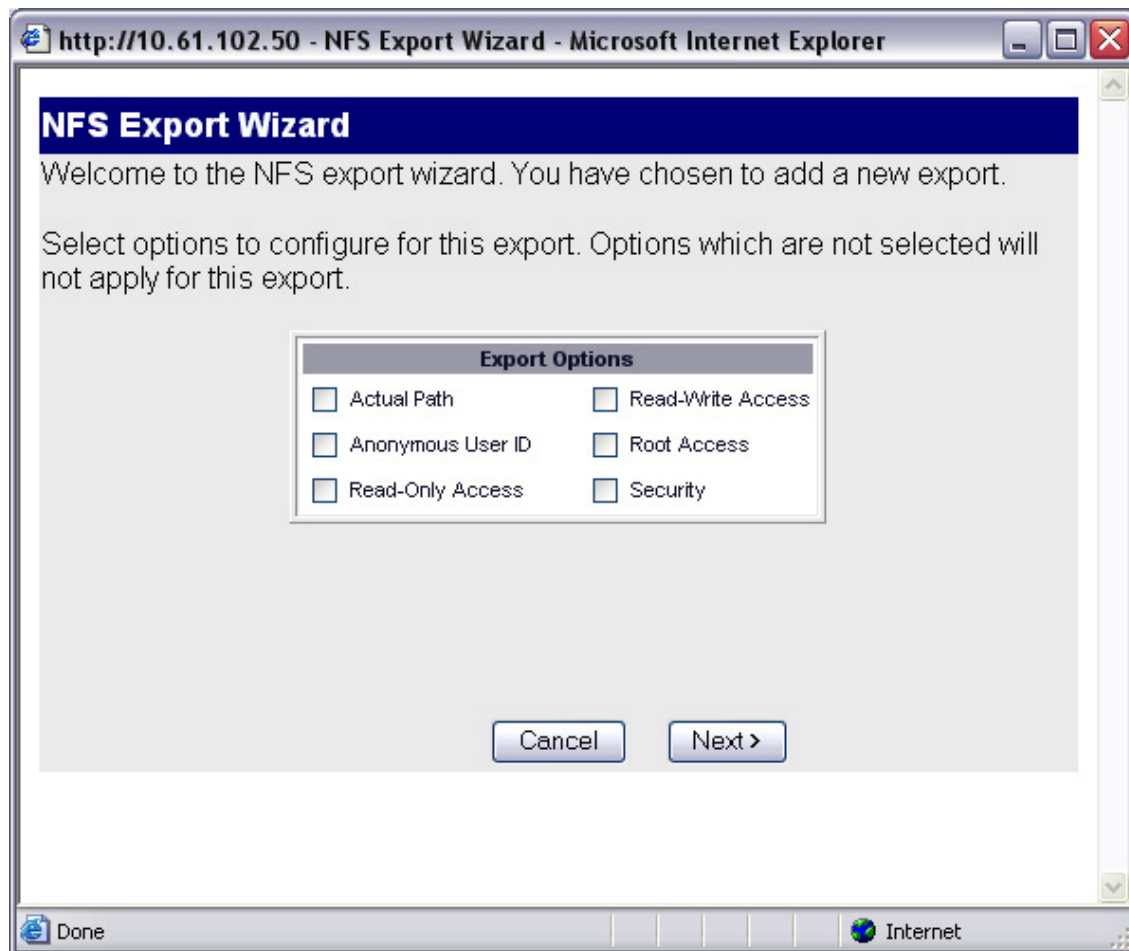


Рис. 11) NetApp NFS Export Wizard.

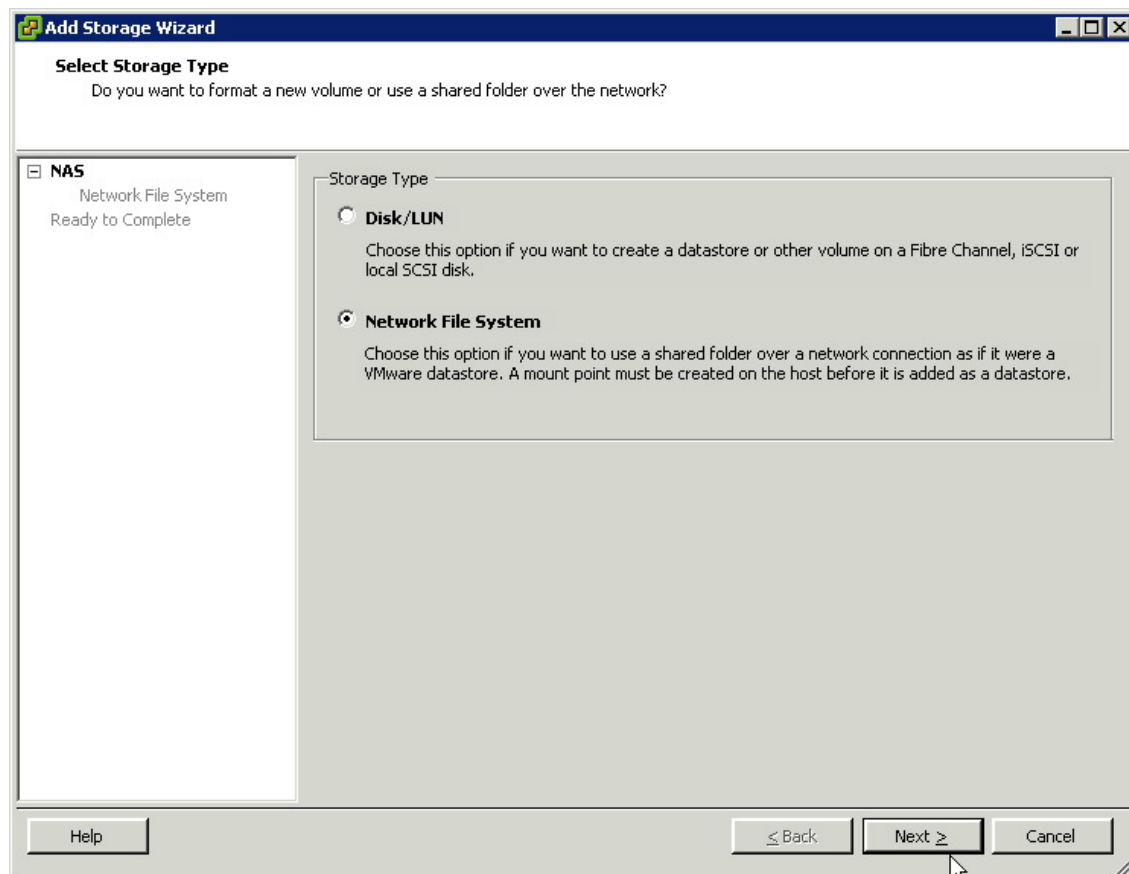


Рис. 12) VMware Add Storage Wizard.

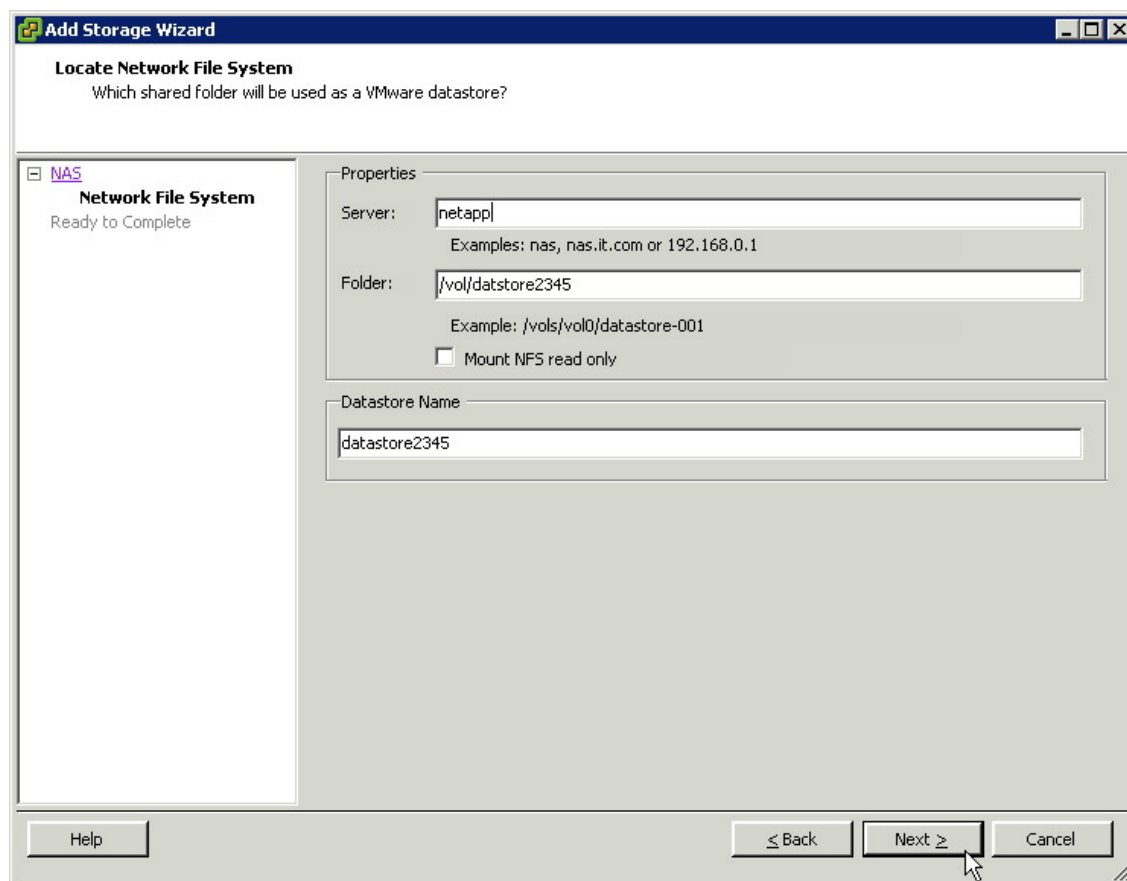


Рис. 13) VMware Add Storage Wizard NFS configuration

Хост ESX 3.5

Для оптимальной настройки NFS Datastores, NetApp рекомендует сделать следующие изменения на каждом хосте ESX 3.5.

- 1 Откройте VirtualCenter.
- 2 Выберите хост ESX.
- 3 В правой панели выберите закладку Configuration.
- 4 В блоке Software, выберите Advanced Configuration.
- 5 В появившемся окне выберите слева NFS.
- 6 Измените значение NFS.HeartbeatFrequency на 12.
- 7 Измените значение NFS.HeartbeatMaxFailures на 10.
- 8 Повторите для каждого сервера ESX.

Хост ESX 3.0

Для оптимальной настройки NFS Datastores, NetApp рекомендует сделать следующие изменения на каждом хосте ESX 3.0.

- 1 Откройте VirtualCenter.
- 2 Выберите хост ESX.
- 3 В правой панели выберите закладку Configuration.
- 4 В блоке Software, выберите Advanced Configuration.
- 5 В появившемся окне выберите слева NFS.

- 6 Измените значение `NFS.HeartbeatFrequency` на 5 с 9.
- 7 Измените значение `NFS.HeartbeatMaxFailures` на 25 с 3.
- 8 Не изменяйте значение `NFS.HeartbeatTimeout` (по умолчанию 5).
- 9 Повторите для каждого сервера ESX.

4.4 ПОДКЛЮЧЕНИЕ СИСТЕМЫ ХРАНЕНИЯ

Этот раздел рассматривает возможные варианты и специфичные настройки ESX 3.5 и рассматривает установки, специфичные для каждой из технологий.

Подключение по Fibre Channel

Во-первых, обратите внимание, что Fibre Channel это единственный протокол доступа к данным, включенный по умолчанию на сервере ESX. NetApp рекомендует иметь на каждом сервере ESX по два FC HBA порта, для целей подключения систем хранения, или как минимум один порт FC HBA, и порт iSCSI (программный или аппаратный), для обеспечения отказоустойчивости и избыточности. Для подключения LUN по FC, воспользуйтесь следующими шагами.

1. Откройте VirtualCenter.
2. Выберите хост ESX.
3. В правой панели выберите закладку Configuration.
4. В поле Hardware, щелкните Storage Adapters.
5. В верхнем правом углу, щелкните Rescan.
6. Повторите шаги с 1 по 5 для каждого сервера ESX.

Выбор Rescan принуждает систему пересканировать все HBA (FC и iSCSI) для обнаружения изменений на системе хранения, подключенной к ESX Server.

Внимание: Некоторые FCP HBA требуют провести сканирование дважды, для обнаружения новых LUN-ов (см. VMware KB1798 <http://kb.vmware.com/kb/1798>). После того, как LUN-ы обнаружены, они могут быть назначены виртуальной машине через raw device mapping, или предоставлены самому ESX Server как datastore.

Чтобы добавить LUN как datastore, сделайте следующее:

1. Откройте VirtualCenter.
2. Выберите хост ESX.
3. В правой панели выберите закладку Configuration.
4. В поле Hardware, выберите Storage и щелкните Add Storage, чтобы открыть Add Storage Wizard. См. рис. 14.
5. Выберите радиокнопку Disk/LUN и нажмите Next.
6. Выберите LUN, который вы хотите использовать и нажмите Next.
7. Введите имя datastore и нажмите Next.
8. Выберите block size, нажмите Next, и Finish.

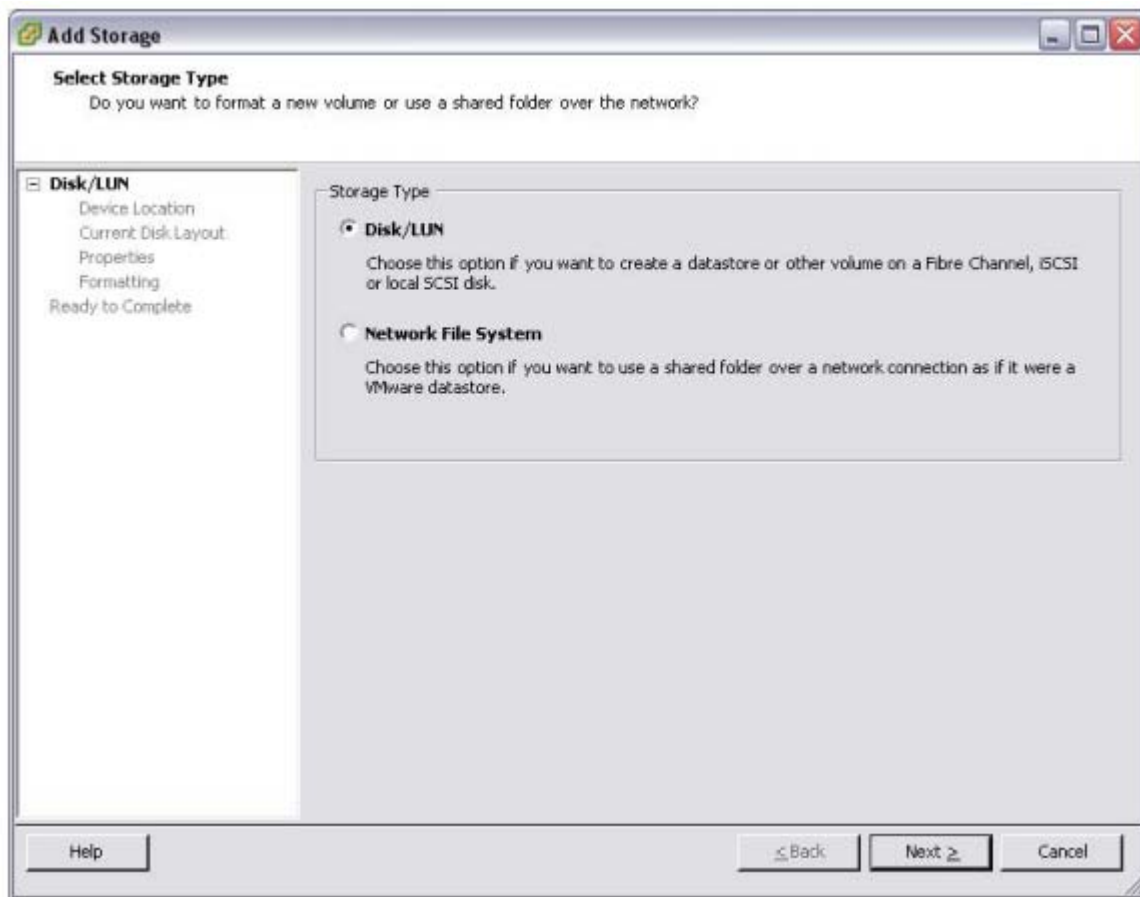


Рис. 14) VMware Add Storage wizard.

Отметьте, что block size по умолчанию для Virtual Machine File System равен 1MB. Такой block size поддерживает хранение файлов виртуальных дисков размером вплоть до 256GB. Если вы планируете хранить в datastore виртуальные диски размером больше 256GB, вам следует увеличить block size установленный по умолчанию. См. рис. 15.

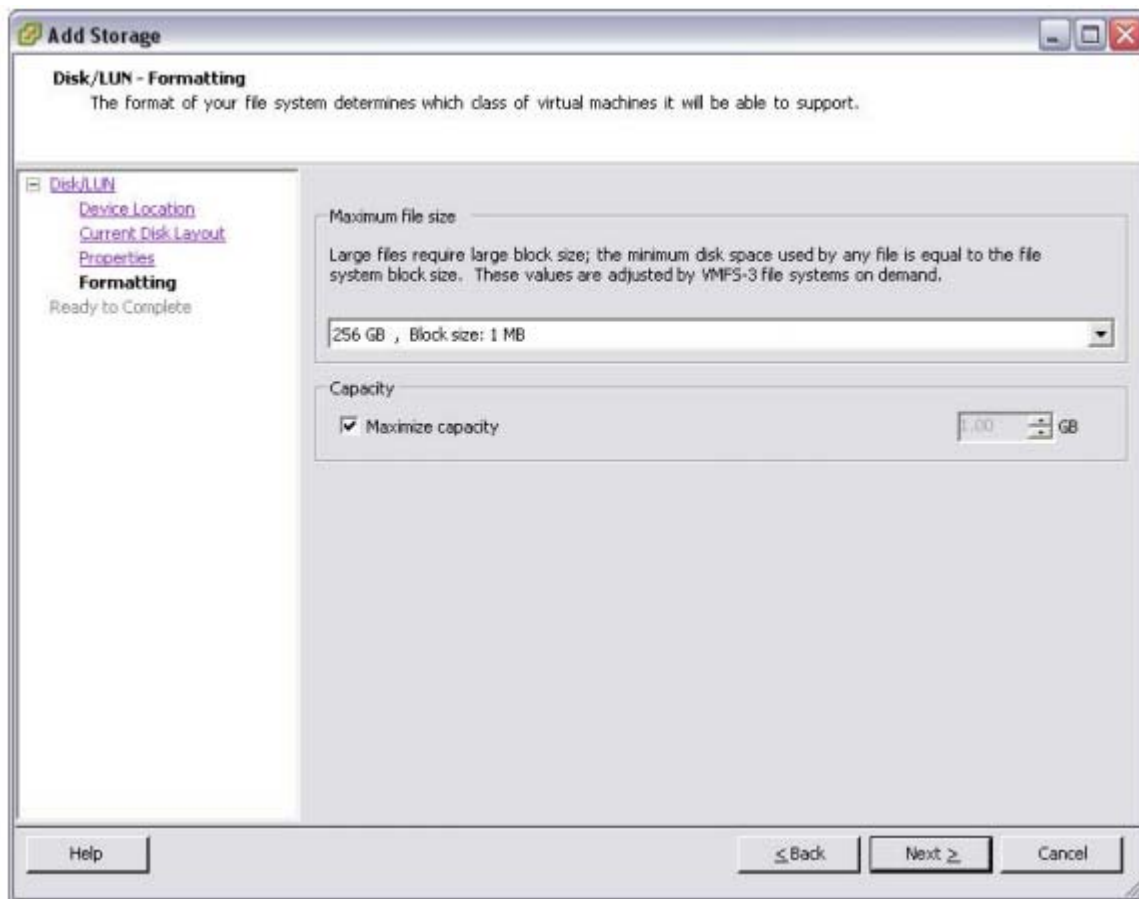


Рис. 15) Форматирование LUN с VMFS.

Подключение по iSCSI/IP SAN

Как наиболее правильное решение, NetApp рекомендует отделить трафик iSCSI от всего прочего сетевого IP трафика, используя отдельную физическую сеть, или VLAN. Такая схема позволит защитить полосу пропускания, доступную для сети хранения, равно как и данные FC или iSCSI не будут влиять на трафик общей сети IP.

Для создания второй сети в ESX, требуется создать второй vSwitch, другой, чем используемый для трафика виртуальных машин. Для включения IP-сети хранения, сервер ESX требует порт Vmkernel, определенный на этом vSwitch. NetApp рекомендует, чтобы каждый имел service console port, заданный на vSwitch, который будет использован в сети общего трафика виртуальных машин, и второй, на vSwitch, используемом только под трафик IP-сети хранения. Второй service console port добавляется для обеспечения отказоустойчивого избыточного подключения в архитектуре ESX HA.

Дополнительную безопасность может обеспечить запрет IP-сети хранения маршрутизировать трафик в общую сеть и наоборот. Если ваша сеть сконфигурирована таким образом, то отметьте, что service console port в сети хранения обеспечивает избыточность только для событий ESX HA. Он не обеспечивает доступ к управлению ESX, в случае полной потери доступа к service console port, подключенного к общей сети.

Работоспособность IP-сети хранения, или Vmkernel, может быть проверена командой vmkping. В случае LUN, подключенного по iSCSI, синтаксис текстовой команды будет: vmkping <iSCSI target>.

Для того чтобы сконфигурировать подключение по iSCSI следуйте таким шагам:

1. Откройте VirtualCenter
2. Выберите хост ESX

3. В правой панели выберите закладку Configuration
4. В блоке Hardware выберите Networking
5. В верхнем правом углу щелкните Add Networking, чтобы открыть Add Network Wizard (см. Рис. 16)
6. Выберите радиокнопку VMkernel и нажмите Next
7. Выберите существующий VMkernel или создайте новый
Внимание: Если отдельная iSCSI-сеть еще не существует, то создайте новый.
8. Нажмите Next
9. Введите IP-адрес и маску подсети, нажмите Next и Finish, чтобы завершить Add Network Wizard (см. Рис. 17)
10. Дополнительно: В случае VMkernel IP-storage network шлюз по умолчанию (default gateway) вводить не обязательно. (см. Рис. 17)
11. В закладке Configuration, левой части, выберите Security Profile
12. В правой части, выберите линк Properties, чтобы открыть окно Firewall Properties.
13. Выберите чекбокс Software iSCSI Client и нажмите ОК, чтобы закрыть окно Firewall Properties. (см. Рис. 18)
14. В правой панели, блоке Hardware, выберите Storage Adapters.
15. Выделите iSCSI Adapter и кликните линк Properties в блоке Details (см. Рис. 19)
16. Выберите закладку Dynamic Discovery в блоке iSCSI Initiator Properties.
17. Щелкните Add и введите IP-адрес интерфейса в NetApp FAS, на котором разрешен iSCSI.
18. Для дополнительной безопасности выберите закладку CHAP и сконфигурируйте аутентификацию по CHAP. NetApp рекомендует установить и проверить доступ по iSCSI прежде чем включать CHAP-аутентификацию.

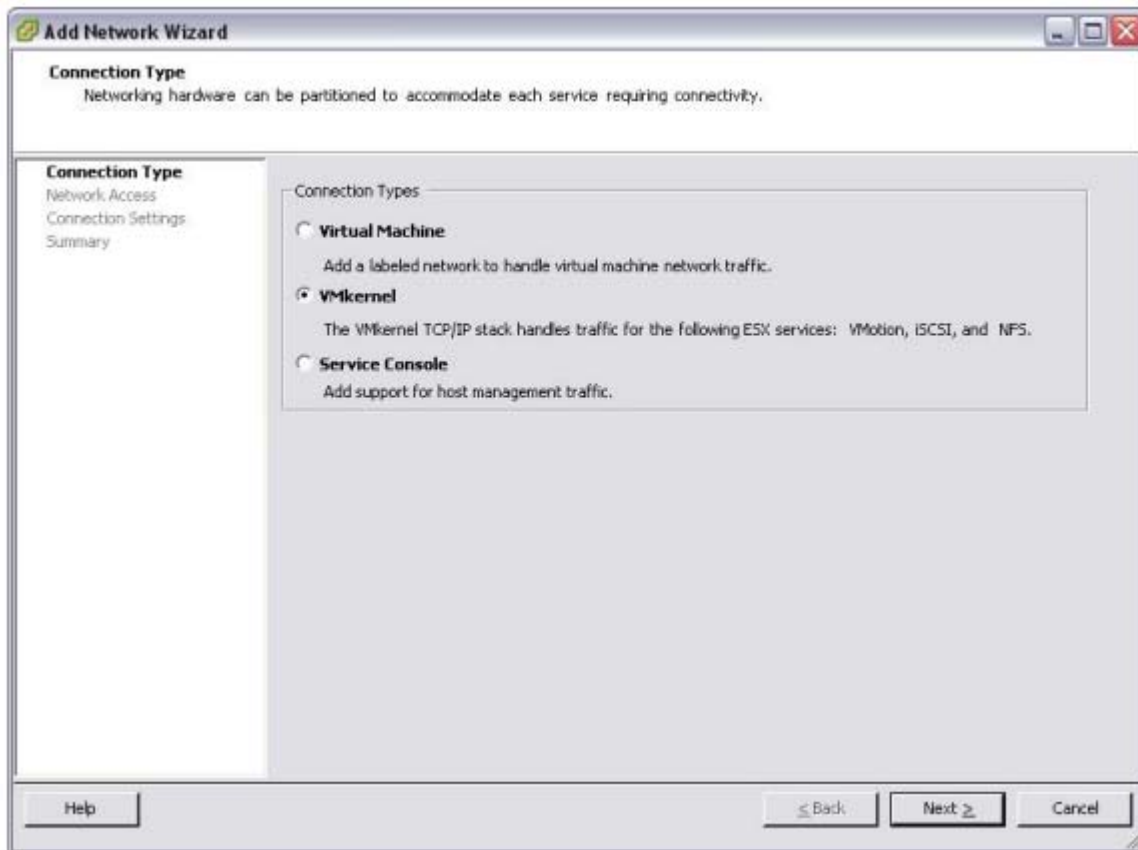


Рис. 16) Добавление порта VMkernel.

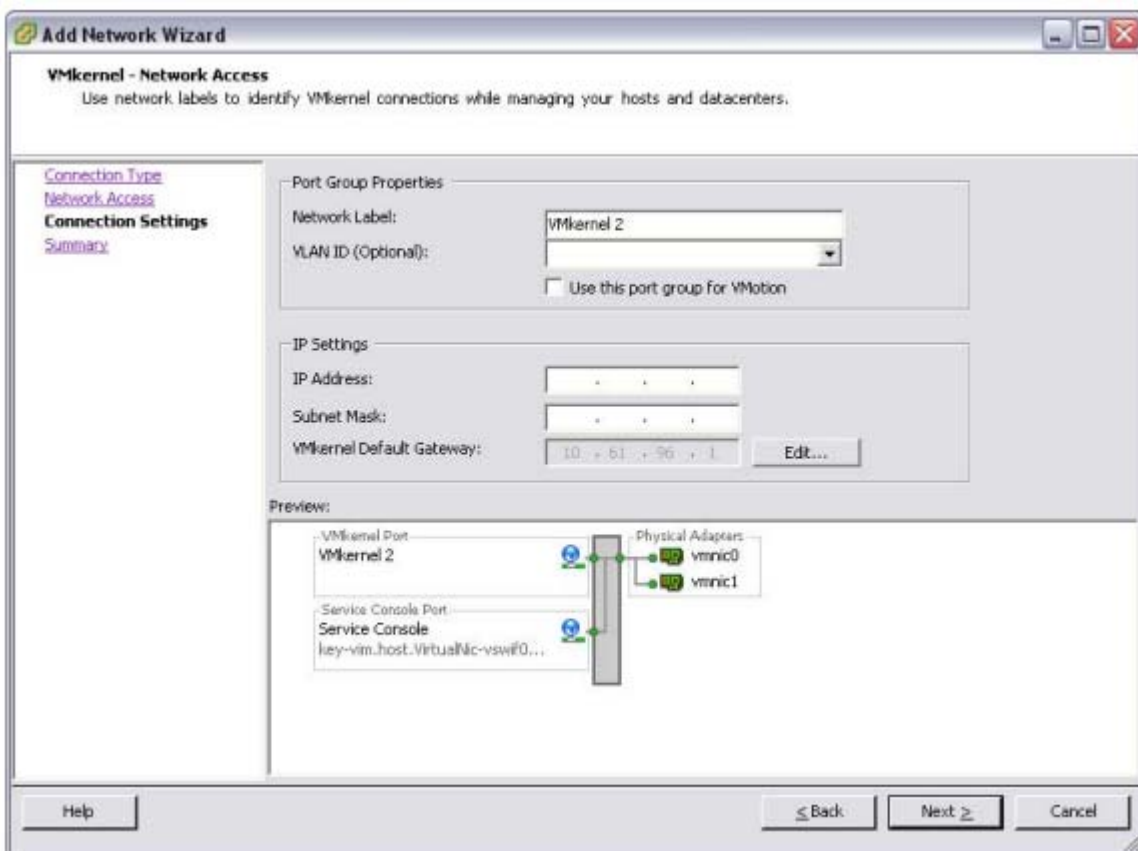


Рис. 17) Конфигурирование порта VMkernel.

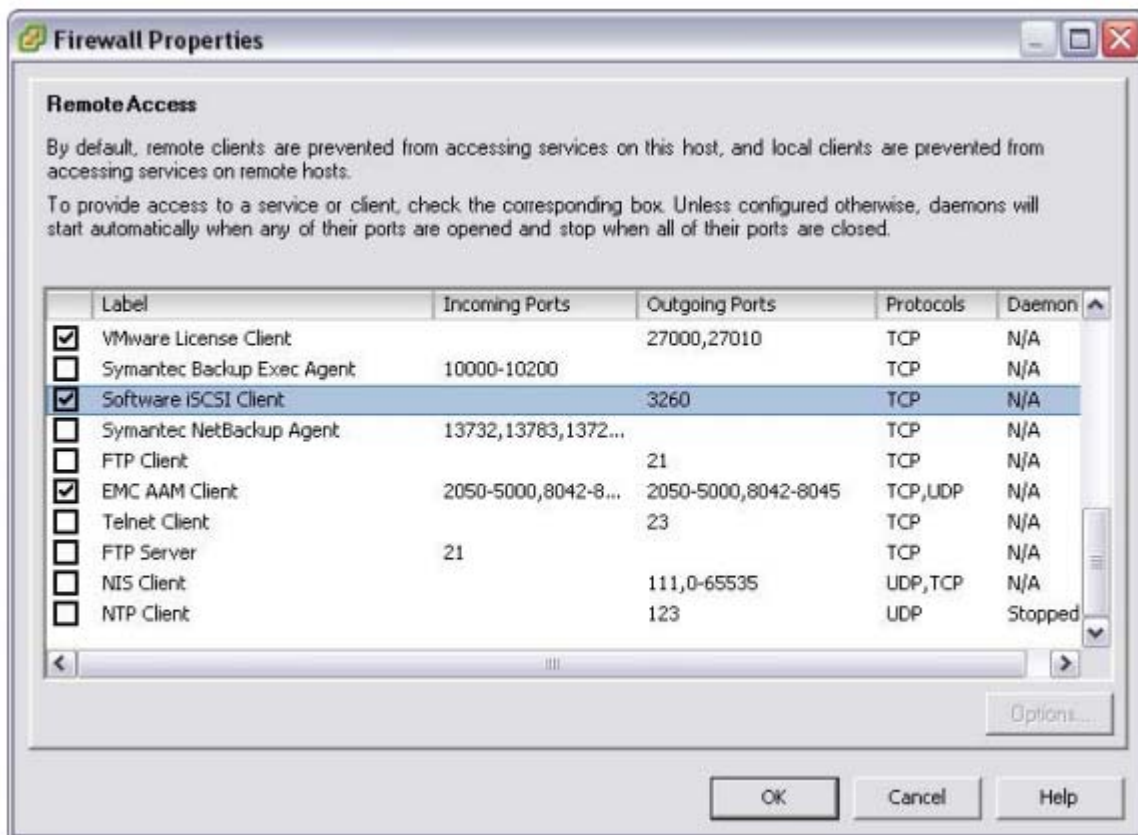


Рис. 18) Конфигурирование firewall в ESX.

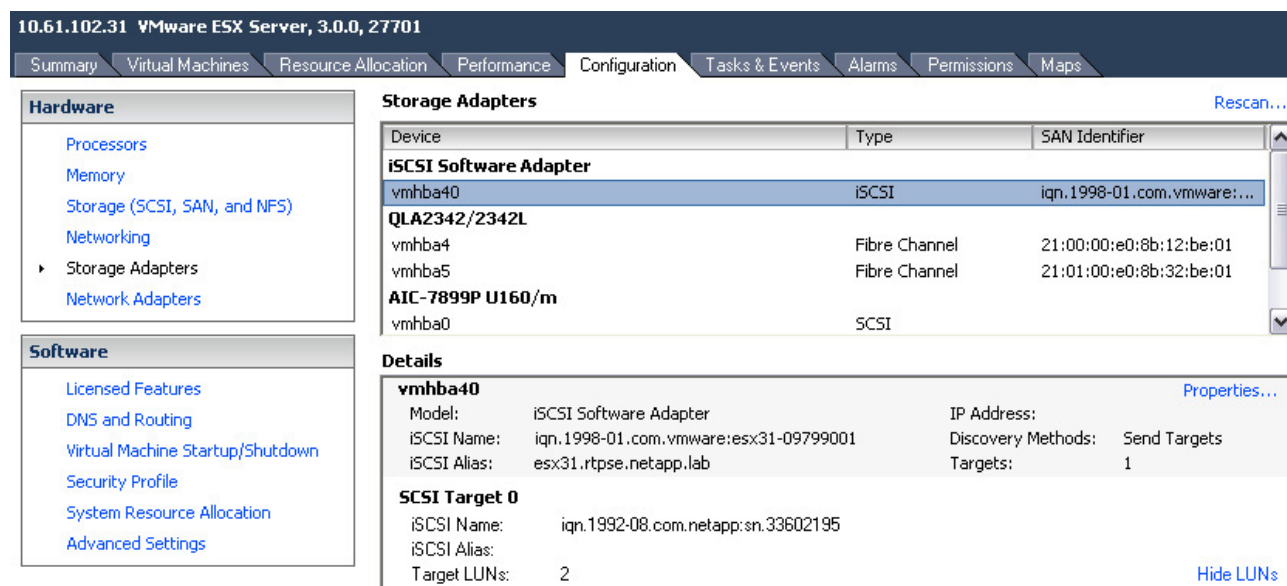


Рис. 19) Выбор iSCSI initiator.

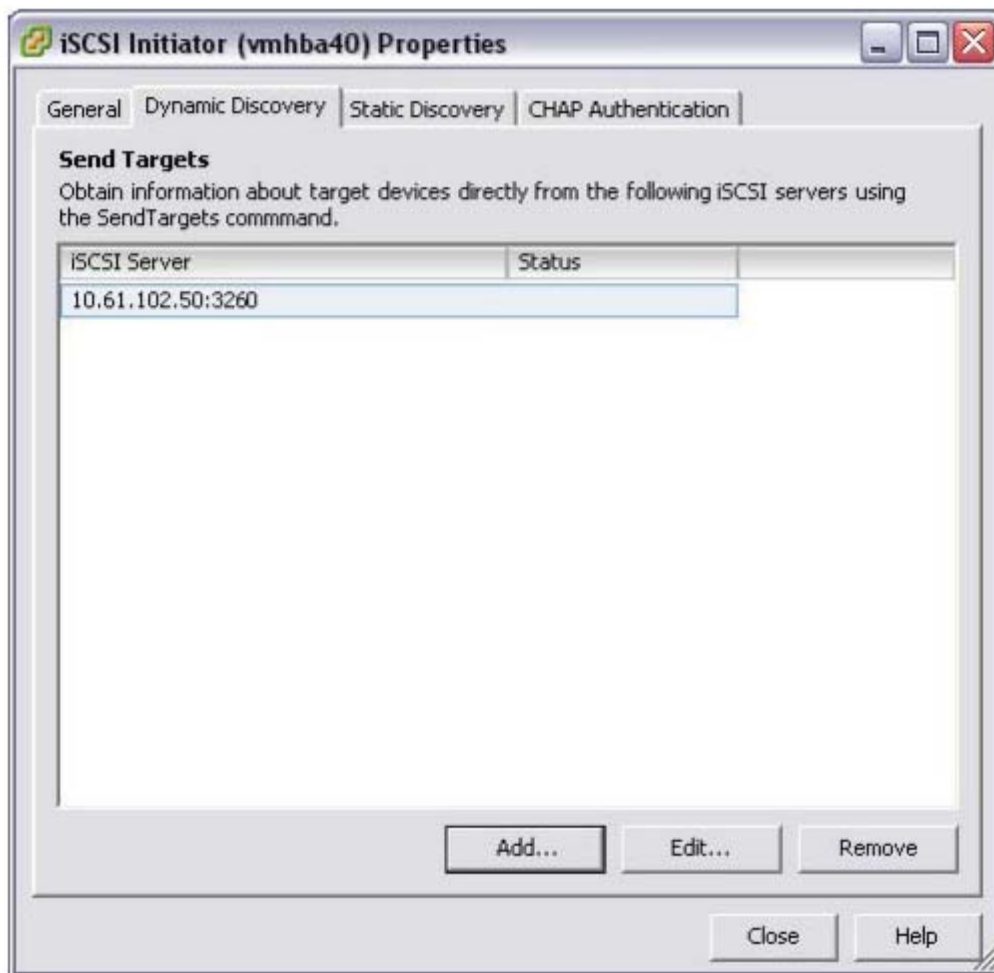


Рис. 20) Конфигурирование iSCSI dynamic discovery.

Если вы пока не готовы использовать iSCSI как ваш основной протокол доступа к данным, вы можете использовать его в различных вспомогательных целях.

С помощью iSCSI можно подключить Datastores, которые хранят образы CD-ROM ISO. Он может быть также использован как избыточный, запасной путь на случай выхода из строя основного пути данных по Fibre Channel. Если вы используете такой вариант, то вы должны сконфигурировать LUN multipathing. Смотрите **Multipathing подключение NetApp по Fibre Channel** далее в этой главе. Кроме этого, установка аппаратного iSCSI HBA в сервер ESX, позволит этому серверу загружаться из iSCSI IP SAN.

Подключение по NFS

Как наилучшее решение NetApp рекомендует отделять трафик IP-сети хранения от обычного IP-трафика с помощью выделения его в отдельный физический сегмент, или сегмент VLAN. Такая схема защищает полосу пропускания, доступную для сети хранения, подобно тому, как подключение FC не влияет на обычный трафик IP.

Для создания второй сети в ESX, требуется создать второй vSwitch, другой, чем используемый для трафика виртуальных машин. Для включения IP-сети хранения, сервер ESX требует порт Vmkernel, определенный на этом vSwitch. NetApp рекомендует, чтобы каждый имел service console port, заданный на vSwitch, который будет использован в сети общего трафика виртуальных машин, и второй, на vSwitch, используемом только под трафик IP-сети хранения. Второй service console port добавляется для обеспечения отказоустойчивого избыточного подключения в архитектуре ESX HA.

Дополнительную безопасность может обеспечить запрет IP-сети хранения маршрутизировать трафик в общую сеть и наоборот. Если ваша сеть сконфигурирована таким образом, то

отметьте, что service console port в сети хранения обеспечивает избыточность только для событий ESX HA. Он не обеспечивает доступ к управлению ESX, в случае полной потери доступа к service console port, подключенного к общей сети.

Подключение к IP-сети хранения, или VMkernel, может быть проверена с помощью команды `vmkping`. При подключении по NFS, синтаксис команды будет: `vmkping <datastore IP address>`.

Multipathing-подключение NetApp по Fibre Channel

Кластерные системы хранения NetApp FAS имеют опцию, известную как `cfmode`, которая управляет поведением портов Fibre Channel системы, в случае кластерного файловера. Если вы используете кластерное решение NetApp, для подключения системы хранения к VMware, вы должны убедиться, что `cfmode` установлен или в режим **Standby** или в **Single System Image**. Режим **Standby** поддерживается FCP хостами VMware, Windows, Linux, и Solaris™. **Single System Image** поддерживается всеми FCP хостами. Для полного списка поддерживаемых ESX конфигураций FCP, смотрите **NetApp SAN Support Matrix**.

Для проверки текущего состояния `cfmode`, следуйте шагам:

1. Войдите в системную консоль FAS (через SSH, Telnet, или кабель консоли).
2. Введите `fcshow cfmode`.
3. Если `cfmode` необходимо изменить, введите `fcset cfmode <mode type>`.

Режим `cfmode Standby` может требовать больше портов на FC-свитче, так как `multipathing failover` обеспечивается системой хранения и организован через активные/неактивные порты. **Single System Image** требует дополнительного конфигурирования `multipathing` на сервере VMware server. Для дополнительной информации о различных доступных режимах `cfmode`, и влиянии переключения между этим режимами, см. раздел 8 в **Data ONTAP Block Management Guide**.

Multipathing-подключение в VMware для Fibre Channel и iSCSI

Если вы выбрали режим `cfmode Single System Image`, то вам следует сконфигурировать `multipathing` подключение в ESX. При использовании `multipathing` подключения, VMware требует указать `default path` для каждого LUN, подключенного к ESX Server.

Для установки этого пути, следуйте шагам:

1. Откройте VirtualCenter.
2. Выберите ESX Server.
3. В правой панели выберите закладку Configuration.
4. В поле Hardware выберите Storage.
5. В поле Storage, выберите storage и щелкните Properties. См. рис. 21.
6. В диалоге Properties, нажмите кнопку Manage Paths.
7. Определите путь, который вы хотите установить как первичный активный и нажмите кнопку Change. См. рис. 22.
8. В окне Change Path State, выберите путь как Preferred и Enabled и нажмите OK. См. рис. 23.

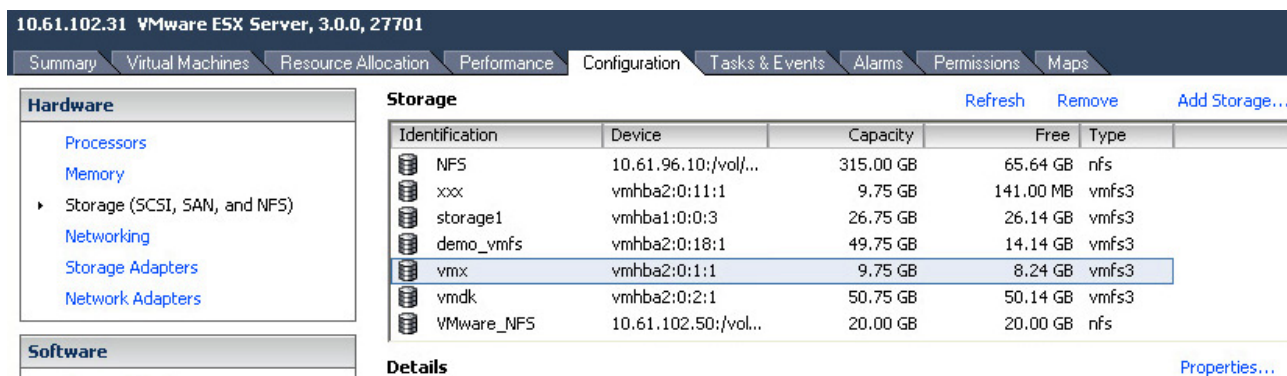


Рис. 21) Выбор Datastore.



Рис. 22) VMware Manage Paths dialog box.

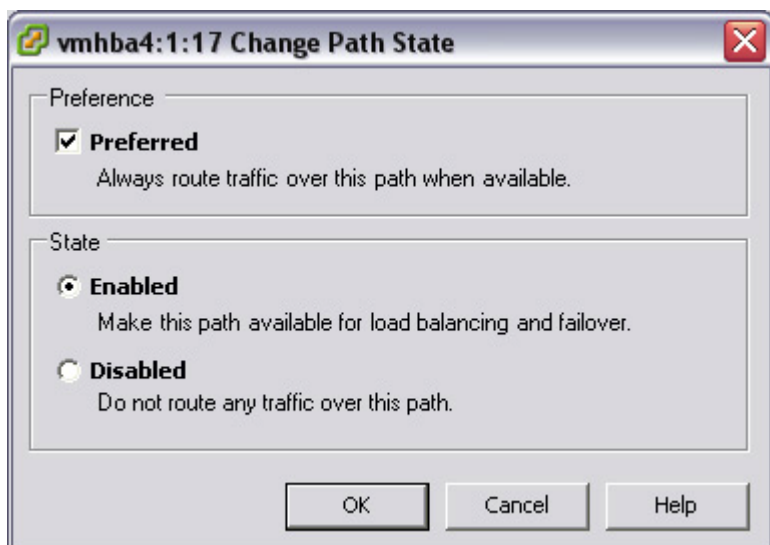


Рис. 23) Установка настроек пути.

Другой метод установки предпочтительного пути для нескольких LUN, это использовать VirtualCenter. Этот метод устанавливает предпочтительный путь для нескольких LUN. Для выполнения следуйте шагам.

1. Откройте VirtualCenter.
2. Выберите ESX Server.
3. В правой панели выберите закладку Configuration.
4. В поле Hardware выберите Storage Adapters.
5. В панели Storage Adapters выберите host bus adapter.

6. Выделите все LUN, которые вы хотите сконфигурировать.
7. Правым щелчком кликните на выделенных LUN-ах и выберите Manage Paths. См. рис. 24.
8. В окне Manage Path, установите политику multipathing и предпочтительный путь для всех выделенных LUN-ов. См. рис. 25.

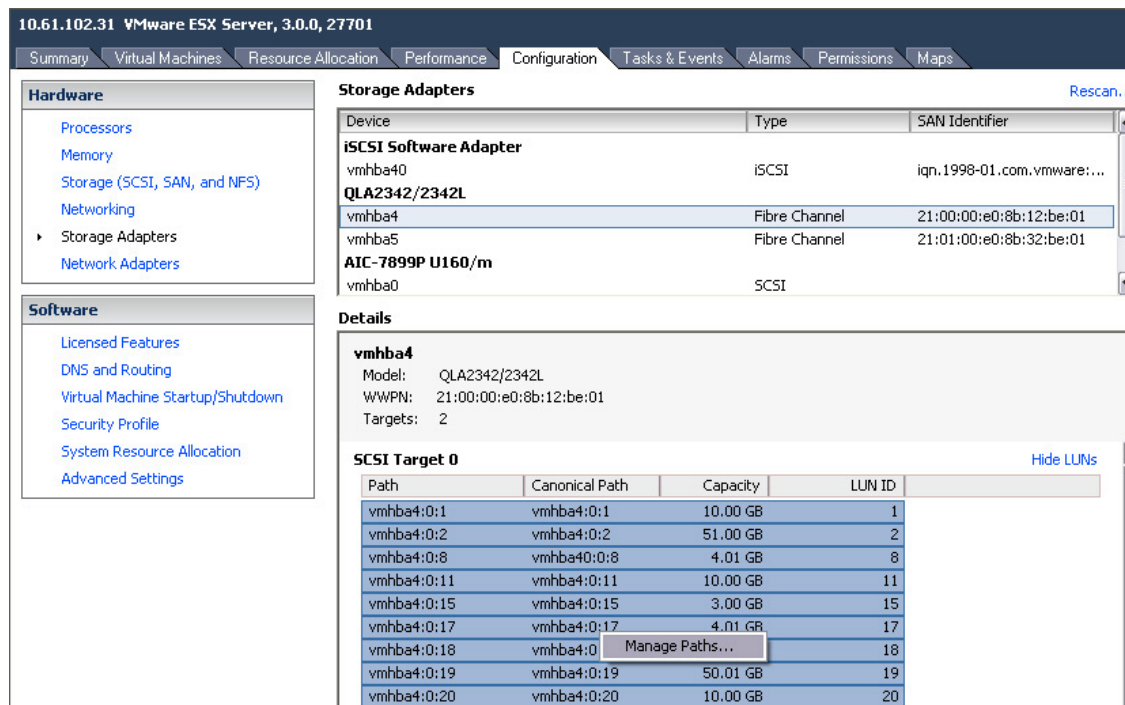


Рис. 24) Выбор SCSI targets.

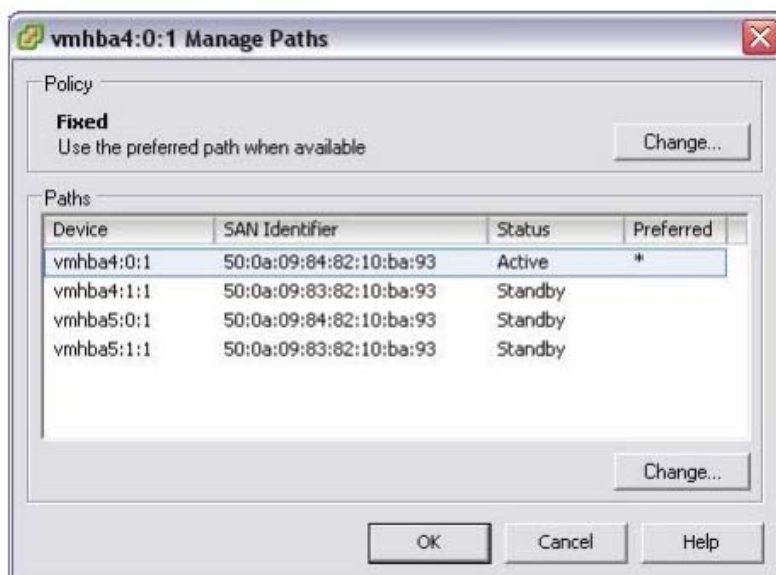


Рис. 25) Установка предпочтительного пути.

Multipathing-подключение с помощью NetApp ESX Host Utilities

NetApp разработал инструмент для упрощения управления узлами ESX в FC SAN. Этот инструмент есть набор скриптов и программ, называющийся FCP ESX Host Utilities for Native OS.

Один из компонентов Host Utilities это скрипт, называющийся config_mpath. Этот скрипт уменьшает нагрузку администратора по управлению путями SAN, используя ранее описанные процедуры. Скрипт config_mpath может определить желаемый первичный путь

к каждому LUN на ESX Server, и установить предпочтительный. Конфигурирование multipathing подключения для множества LUN может быть выполнено быстро и просто, с помощью запуска скрипта `config_mpath` один раз на всех серверах ESX входящих в датацентр. Если делаются изменения в конфигурации системы хранения, то достаточно еще раз запустить скрипт, для обновления конфигурации на основе сделанных изменений. Другая полезная часть инструмента FCP ESX Host Utilities for Native OS это скрипт `config_hba`, который устанавливает настройки HBA timeout, и делает некоторые другие настройки, нужные для работы с системами хранения NetApp, а также набор скриптов, используемых для сбора конфигурационной информации, в случае обращения в техподдержку с проблемами.

Для дополнительной информации о FCP ESX Host Utilities for Native OS, смотрите **NetApp SAN/iSAN compatibility guide**

5. НАИЛУЧШИЕ РЕШЕНИЯ IP-СЕТИ ХРАНЕНИЯ

NetApp рекомендует использовать выделенные ресурсы для трафика передачи данных всегда, когда это возможно. В случае IP-сети хранения, это может быть достигнуто с помощью отдельных физических коммутаторов, или логически, с помощью VLAN в общей коммутируемой сетевой инфраструктуре IP.

10 GB Ethernet

VMware ESX 3 и ESXi 3 представили поддержку 10 Gb Ethernet. Преимущества 10 GbE это возможности использовать меньше сетевых портов в инфраструктуре, в особенности, но не только, для blade-серверов. Для того, чтобы проверить наличие поддержки для вашего оборудования, смотрите **VMware ESX I/O compatibility guide**

VLAN ID

Когда сетевой трафик сегментируется с использованием VLAN-ов, интерфейсы могут как быть выделены для конкретного VLAN, так и поддерживать несколько VLAN-ов с использованием VLAN tagging. Для систем с небольшим количеством NIC, таких как blade-сервера, использование VLAN-ов может быть очень удобно. Объединение двух NIC-ов вместе обеспечивает серверу ESX физическую избыточность сетевых линков. Добавлением нескольких VLAN-ов, можно сгруппировать общий трафик IP по нескольким отдельным VLAN-ам для оптимизации производительности. Рекомендуется объединить доступ к Service console с Virtual Machine Network в один VLAN, и во второй VLAN поместить трафик VMkernel и VMotion. VLAN-ы и VLAN tagging играют важную роль в обеспечении безопасности IP-сети хранения. Экспорты NFS могут быть ограничены диапазоном IP-адресов, доступных только VLAN сети хранения. NetApp также поддерживает ограничение для протокола iSCSI определенными интерфейсами и/или VLAN tags.

Эти простые настройки конфигурации дают огромный эффект в обеспечении безопасности и доступности Datastores в IP-сети хранения. Если вы используете несколько VLAN-ов на одном и том же интерфейсе, убедитесь, что у вас на нем есть достаточный запас по пропускной способности для всего запланированного трафика.

Виртуальные интерфейсы NetApp

Виртуальный сетевой интерфейс (virtual network interface, VIF) это механизм, поддерживающий агрегирование сетевых интерфейсов в один логическое интерфейсное устройство. Будучи создан, VIF не отличается от физического сетевого интерфейса. VIF используется для создания отказоустойчивого сетевого соединения, и, в некоторых случаях, повышения производительности и пропускной способности системы хранения.

Multimode VIF совместим с IEEE 802.3ad. В режиме multimode VIF, все физические соединения, входящие в VIF одновременно активны и передают данные. Это режим требует, чтобы все соединения, входящие в VIF были подключены в коммутатор, поддерживающий транкинг или агрегацию по нескольким портам. Коммутатор должен быть сконфигурирован так, чтобы понимать, что все порты соединения используют один и тот же MAC-адрес, и они часть одного логического интерфейса.

В режиме single-mode VIF, только одно физическое соединение активно в каждый момент времени. Если контроллер системы хранения обнаруживает отказ в активном соединении, активируется запасное соединение. Для использования single-mode VIF не требуется настройка коммутатора, и физические интерфейсы, составляющие VIF, не соединяются с одним и тем же коммутатором. Отметьте, что IP load balancing не поддерживается для single-mode VIF.

Также возможно создать single или multimode VIF второго уровня. Используя VIF второго уровня можно получить преимущества от одновременного использования как увеличения

пропускной способности и балансировки multimode VIF, так и отказоустойчивых возможностей single-mode VIF. В этой конфигурации, создаются два multimode VIF, каждый на отдельный коммутатор. Затем создается single-mode VIF, состоящий из двух multimode VIF-ов. При нормальной работе трафик идет через только один multimode VIF; но в случае отказа или отключения коммутатора, контроллер системы хранения переносит трафик на другой multimode VIF.

Использование коммутаторов Ethernet

Инфраструктура IP-сети обеспечивает необходимую гибкость подключения к системе хранения различными способами в зависимости от ваших потребностей. Базовая архитектура может обеспечить один избыточный линк к Datastore, достаточный для хранения, например ISO images, различных резервных копий или шаблонов VM. Избыточная архитектура, применяемая на большинстве рабочих систем, имеет по несколько линков, обеспечивающих отказоустойчивость для коммутаторов и сетевых интерфейсов.

Средства агрегации линков и балансировки нагрузки, применяемые при одновременном использовании нескольких коммутаторов и интерфейсов, обеспечивают отказоустойчивость и дополнительное повышение пропускной способности сетевой инфраструктуры.

Некоторые коммутаторы Ethernet поддерживают так называемый «stacking» (стекирование), когда несколько коммутаторов объединяются высокоскоростным соединением, позволяющим использовать более широкую полосу пропускания между коммутаторами. Некоторые стекируемые коммутаторы поддерживают так называемые транки типа «cross-stack Etherchannel», когда интерфейсы на физически разных коммутаторах могут быть объединены по стандарту 802.3ad Etherchannel trunk, распределенном по нескольким коммутаторам. Преимущества cross-stack Etherchannel trunks в том, что отсутствует необходимость дополнительных пассивных линков, требуемых в некоторых конфигурациях для обеспечения отказоустойчивости.

Все конфигурации IP-сети хранения, рассмотренные здесь, используют избыточные Ethernet-коммутаторы и интерфейсы для обеспечения необходимой отказоустойчивости инфраструктуры VMware.

Конфигурация для рабочей IP-инфраструктуры сети хранения

Одна из задач, которая должна быть решена при конфигурировании сетевой IP-инфраструктуры хранения VMware ESX, это то, что сетевая конфигурация должна соответствовать одновременно нескольким требованиям:

- Иметь избыточные подключения к коммутаторам при многокоммутаторной структуре
- Иметь столько физических путей передачи, сколько возможно
- Масштабироваться по нескольким физическим интерфейсам

6. ВАРИАНТЫ КОНФИГУРАЦИИ СЕТИ VMWARE ESX

6.1 СОЗДАНИЕ ВЫСОКОДОСТУПНОЙ IP-СЕТИ ХРАНЕНИЯ С ТРАДИЦИОННЫМИ КОММУТАТОРАМИ ETHERNET

Введение в конфигурацию с несколькими портами VMkernel

Для того, чтобы одновременно использовать несколько путей передачи данных, для обеспечения отказоустойчивости с традиционными коммутаторами Ethernet, каждый сервер ESX должен быть сконфигурирован, как минимум, с двумя портами VMkernel на одном и том же VSwitch.

Этот VSwitch конфигурируется с, как минимум, двумя сетевыми адаптерами. Каждый из этих портов VMkernel поддерживает трафик IP в отдельную подсеть. Так как два порта VMkernel идут в один VSwitch, они могут разделять физический сетевой адаптер в этом VSwitch.

Описание поведения адаптеров сервера ESX в случае отказа

В случае отказа адаптера в ESX server (по причине обрыва кабеля или выхода из строя NIC), трафик, изначально шедший через сбойный адаптер, перемаршрутизируется и продолжает идти через другой адаптер, но в ту же подсеть, что и у исходного адаптера.

Обе подсети работают на оставшемся физическом адаптере. Трафик возвращается на исходный адаптер, когда адаптер возвращается в работу.

Отказ коммутатора Ethernet

Трафик, изначально шедший на сбойный коммутатор, перемаршрутизируется и продолжает идти через другой адаптер, через работающий коммутатор на контроллер системы хранения. Трафик возвращается на исходный адаптер, когда коммутатор, к которому он подключен, возвращается в работу.

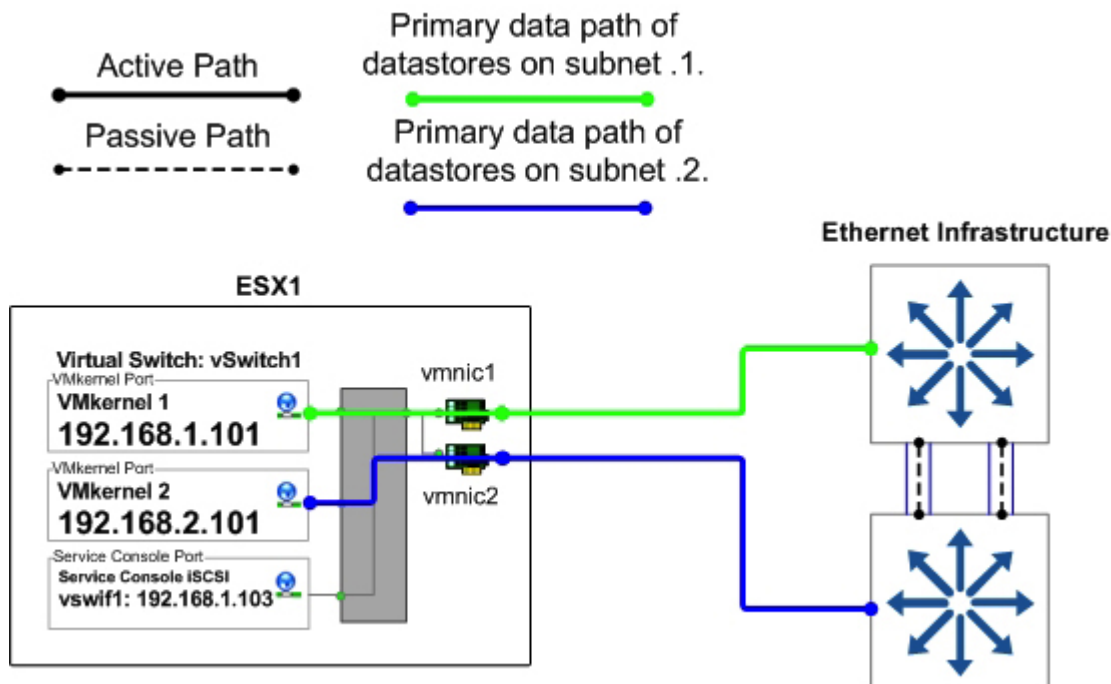


Рис. 26) Нормальная работа ESX vSwitch1.

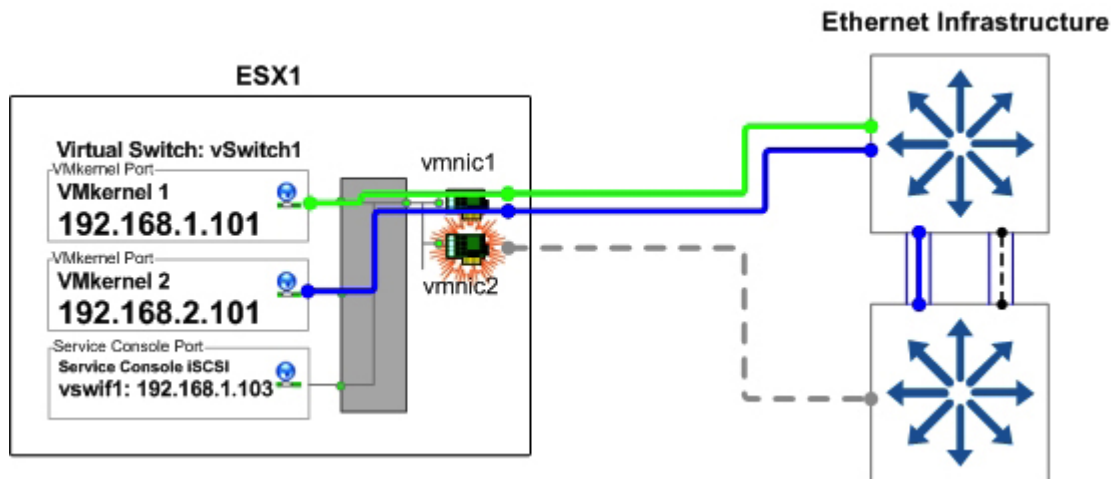


Рис. 27) Работа при сбое ESX vSwitch1.

Масштабируемость сетевых соединений сервера ESX

Хотя конфигурация, показанная на рисунке выше, использует только два сетевых адаптера на каждом сервере ESX, число их может быть увеличено, с добавлением дополнительных VMkernel port, подсетей и IP-адресов для каждого дополнительного адаптера.

Другой вариант, это добавить третий адаптер, и сконфигурировать его как запасной адаптер на случай отказа вида N+1. Но, не добавляя порты VMkernel или IP-адреса, третий адаптер может быть сконфигурирован как standby port для обоих портов VMkernel. В этом случае, если один из основных физических адаптеров отказывает, то третий адаптер занимает его место, принимая трафик, шедший на сбойный адаптер, обеспечивая отказоустойчивость без снижения потенциальной полосы пропускания в течение сбоя.

6.2 ESX NETWORKING БЕЗ ETHERCHANNEL

Если коммутаторы, используемые для IP-сети хранения, не поддерживают cross-stack Etherchannel trunking, то задача обеспечения межкоммутаторной избыточности (cross-switch redundancy) при активном использовании многопутевого подключения становится довольно непростой. Для обеспечения этого, каждый ESX Server должен быть сконфигурирован с, как минимум двумя портами VMkernel IP, смотрящими в разные подсети. Как и в предшествующем варианте, множественным соединениям от Datastore контроллеру системы хранения необходимо использовать различные target IP-адреса. Без добавления второго VMkernel port, VMkernel будет просто маршрутизировать все исходящие пакеты через один и тот же физический интерфейс, без использования дополнительных VMNIC на vSwitch. В этой конфигурации для каждого VMkernel port устанавливается IP-адрес в отдельную подсеть. Система хранения также конфигурируется с IP-адресами в каждой из этих подсетей, так что использование определенных интерфейсов VMNIC может быть управляемо.

Преимущества

- Обеспечивает два активных соединения для каждого контроллера системы хранения (но только один активный путь на Datastore).
- Легко масштабируется для большего количества соединений.
- Балансировка нагрузки для контроллера системы хранения автоматически управляется политиками Etherchannel IP load balancing policy. Это НЕ Etherchannel.

Недостаток

- Требуется конфигурация с, как минимум двумя портами VMkernel IP storage ports.

В конфигурации сервера ESX, показанной на Рис. 28, vSwitch (с именем vSwitch1) создан специально для соединения IP storage. Два физических адаптера сконфигурированы для этого vSwitch (в данном случае vmnic1 и vmnic2). Каждый из этих адаптеров соединен с отдельным физическим коммутатором.

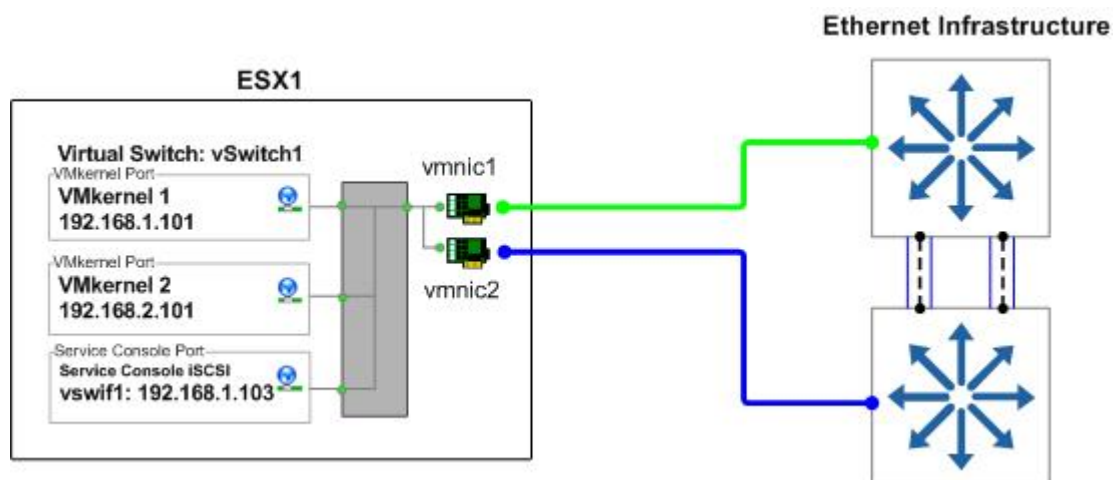


Рис. 28) Соединения физических NIC в ESX Server с традиционным Ethernet.

В vSwitch1, создано два VMkernel ports (VMkernel 1 и VMkernel 2). Каждый VMkernel port сконфигурирован с IP-адресом в отдельную подсеть, и установки NIC Teaming для каждого VMkernel настроены следующим образом:

- VMkernel 1: IP address 192.168.1.101.
- VMkernel 1 Port Properties:
 - Включена опция Override vSwitch Failover Order.
 - Установлен как Active Adapter для vmnic1.
 - Установлен как Standby Adapter для vmnic2.
- VMkernel 2: IP address 192.168.2.101.
- VMkernel2 Port Properties:
 - Включена опция Override vSwitch Failover Order.
 - Установлен как Active Adapter для vmnic2.
 - Установлен как Standby Adapter для vmnic1.

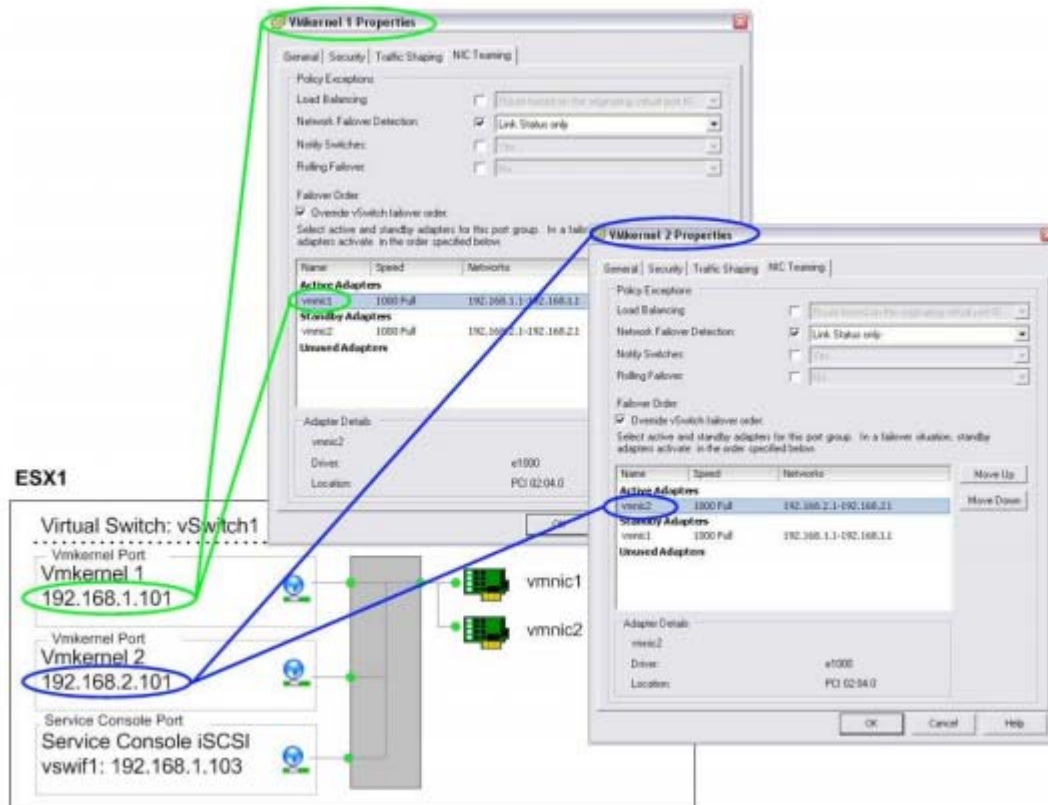


Рис. 29) Свойства VMkernel port в ESX Server с традиционным Ethernet.

6.3 ESX С НЕСКОЛЬКИМИ VMKERNEL, ТРАДИЦИОННЫМ ETHERNET, И NETAPP С SINGLE MODE VIFS

В этой конфигурации, используется коммутатор IP, не поддерживающий cross-stack Etherchannel trunking, поэтому от каждого контроллера системы хранения требуется четыре физических сетевых интерфейса. Интерфейсы делятся на два VIF режима single mode (active/passive). Каждый VIF соединяется с обоими коммутаторами, и использует один IP адрес, ему назначенный, соответственно два IP-адреса на каждый контроллер. Команда `vif favor` используется для того, чтобы принудительно назначить каждому VIF использование соответствующего коммутатора, для его активного интерфейса. Если ваша инфраструктура сети не поддерживает cross-stack Etherchannel, то этот вариант является предпочтительным, так как он прост в реализации и не требует каких-то особенных конфигураций на коммутаторах.

Преимущества

- Не требуется конфигурирование на стороне коммутатора.
- Обеспечивает два активных соединения для каждого контроллера системы хранения.
- Масштабируется для большего числа соединений (требует два физических соединения для каждого активного пути).

Недостатки

- Требует два физических соединения для каждого активного пути.

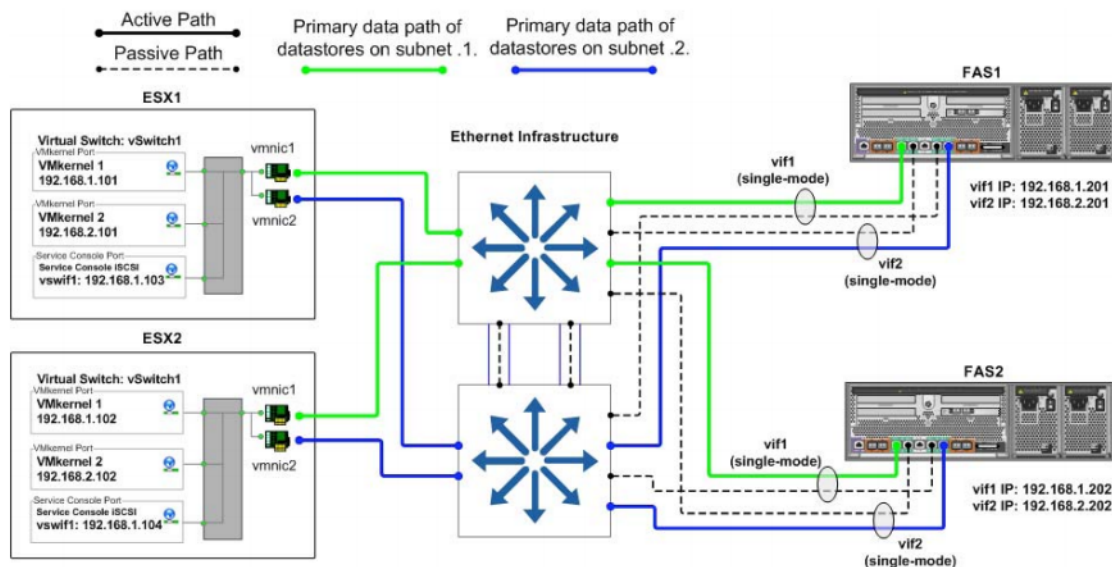


Рис. 30) single-mode VIFs.

6.4 ESX С НЕСКОЛЬКИМИ VMKERNEL, ОБЫЧНЫМ ETHERNET, И NETAPP С MULTI-LEVEL VIFS

Эта конфигурация используется главным образом для создания избыточных путей в случае системы с несколькими коммутаторами, и может быть необходима в случае, когда физические интерфейсы используются, при помощи VLAN tagging, для других протоколов хранения в инфраструктуре. В этой конфигурации используемые коммутаторы IP не поддерживают cross-stack trunking, так что каждому контроллеру системы хранения потребуется четыре физических сетевых соединения. Соединения поделены на два multimode (active/active) VIFs с поддержкой IP load balancing, один VIF соединен с каждым из двух коммутаторов. Эти два VIF объединены в single mode (active/passive) VIF. NetApp называет такую конфигурацию «двухуровневым» (second-level) VIF. Эта опция также требует использования нескольких адресов IP в системе хранения. Несколько адресов IP может быть назначено этому single-mode VIF с помощью алиасов IP-адресов, или с помощью VLAN tagging.

Преимущества

- Обеспечивает два активных соединения для каждого контроллера системы хранения.
- Масштабируется для большего количества соединений (требует два физических линка для каждого активного соединения).
- Балансировка нагрузки для контроллеров автоматически обеспечивается политиками Etherchannel IP load balancing policy.

Недостатки

- Необходима дополнительная настройка на стороне коммутаторов.
- Требует два физических соединения для каждого активного пути.
- Некоторый трафик передачи данных проходит через аплинк между коммутаторами.

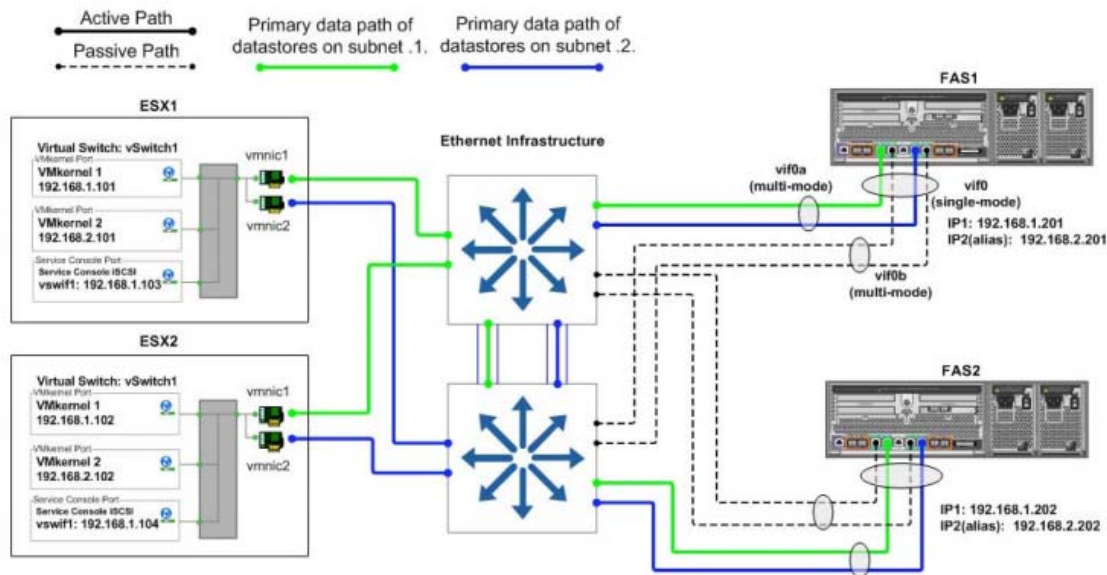


Рис. 31) multimode VIFs на стороне системы хранения.

6.5 КОНФИГУРАЦИЯ DATASTORE С ТРАДИЦИОННЫМ ETHERNET

Дополнительно к правильному конфигурированию vSwitches, сетевых адаптеров и IP-адресов, необходимо использование нескольких одновременно работающих физических линков к сети IP-storage к нескольким Datastores, организуя каждое соединение по отдельному IP-адресу. В дополнение к конфигурированию интерфейсов ESX-сервера, показанному в примере, контроллер системы хранения NetApp конфигурируется с IP-адресом в каждой из подсетей, которая используется для доступа к Datastore. Это осуществляется при использовании соединенных в team нескольких адаптеров, каждого со своим IP-адресом, или, в некоторых сетевых конфигурациях, назначением алиаса IP-адреса для всего team, позволяющих этим адаптерам коммуницировать со всеми нужными подсетями.

При подключении Datastore к серверам ESX, администратор конфигурирует соединение так, чтобы использовать один из IP-адресов, заданных для контроллера NetApp. При использовании NFS Datastores, это осуществляется заданием адреса IP при монтировании Datastore.

Рисунок ниже показывает, как проходит трафик сети хранения, когда используются несколько серверов ESX и несколько Datastores.

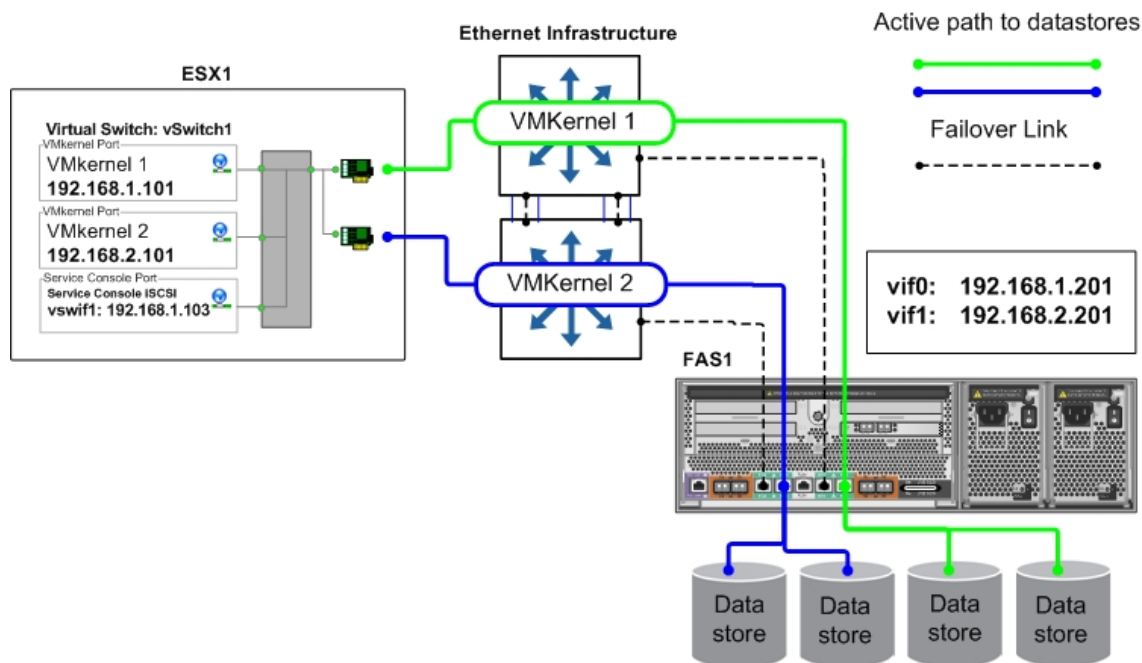


Рис. 32) Соединение с Datastore с помощью традиционного Ethernet.

6.6 IP-ИНФРАСТРУКТУРА ХРАНЕНИЯ ВЫСОКОЙ ДОСТУПНОСТИ С КОММУТАТОРАМИ ETHERNET CROSS-STACK ETHERCHANNEL

Коммутаторы, поддерживающие cross-stack Etherchannel, обеспечивают более простой способ реализовать систему высокой доступности с использованием ESX. Эта глава рассматривает такие варианты.

6.7 ESX NETWORKING И CROSS-STACK ETHERCHANNEL

Если коммутаторы, используемые для построения сети IP storage, поддерживают режим cross-stack Etherchannel trunking, тогда каждому серверу ESX требуется одно физическое подключение к каждому из коммутаторов в стеке с включенной балансировкой нагрузки. Требуется один VMkernel port с одним IP-адресом. Несколько соединений к datastore на контроллере системы хранения, с использованием различных IP-адресов, необходимы при использовании каждого из доступных физических линков.

Преимущества

- Обеспечивает два активных соединения с каждым контроллером системы хранения.
- Легко масштабируется для большего количества соединений.
- Балансировка нагрузки для контроллеров автоматически обеспечивается политиками Etherchannel IP load balancing policy.
- Требуется только одного порта VMkernel на систему хранения при использовании множественных физических линков.

Недостатки

- Требуется поддержки cross-stack Etherchannel на коммутаторе.
- Не все коммутаторы и производители коммутаторов поддерживают cross-switch Etherchannel trunks.

В конфигурации сервера ESX, показанной на рисунке ниже, vSwitch (названный vSwitch1) создан специально для сети IP storage. Два физических адаптера сконфигурированы для этого vSwitch (в данном случае vmnic1 и vmnic2). Каждый из этих адаптеров подключен в

отдельный порт физического коммутатора, и порты коммутаторов объединены при помощи cross-stack Etherchannel trunk. Обратите внимание, что в настоящий момент VMware не поддерживает 802.3ad, или dynamic negotiation для Ethernet trunks.

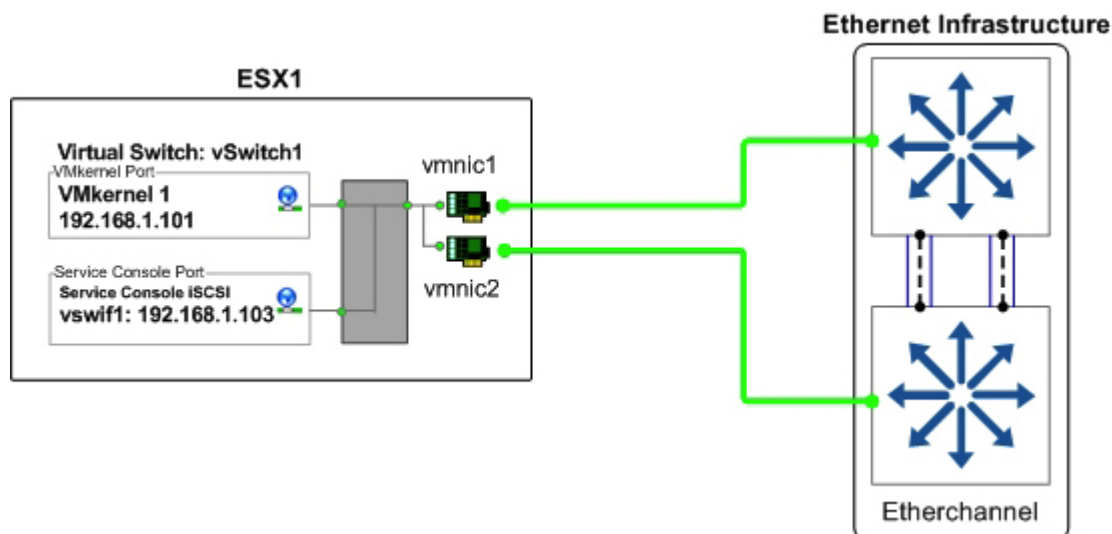


Рис. 33) Физические соединения ESX Server с использованием cross-stack Etherchannel.

В vSwitch1, создан один VMkernel port (VMkernel 1) и сконфигурирован с одним IP-адресом, а свойства NIC Teaming для VMkernel port сконфигурированы следующим образом:

VMkernel 1: IP address установлен 192.168.1.101.

VMkernel 1 Port Properties: политика балансировки установлена на «Route based on IP hash».

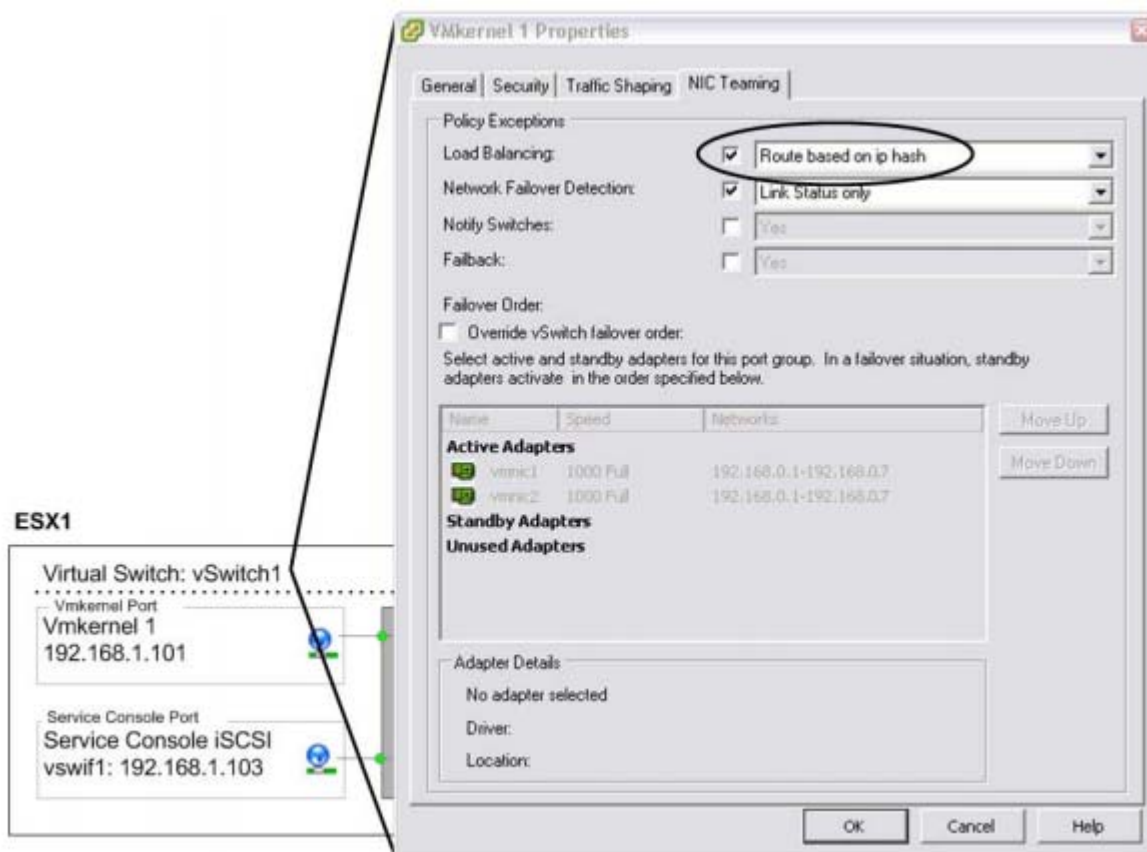


Рис. 34) Свойства VMkernel port в ESX Server с использованием cross-stack Etherchannel.

6.8 ESX, CROSS-STACK ETHERCHANNEL, И NETAPP С MULTIMODE VIFS

Если используемые для работы IP-сети коммутаторы поддерживают cross-stack Etherchannel trunking, то для каждого контроллера системы хранения достаточно одного физического соединения с каждым коммутатором; два порта соединенные с каждым контроллером системы хранения объединяются тогда в один multimode LACP VIF с включенным IP load balancing. Несколько IP-адресов могут быть назначены контроллерам при помощи алиасов в VIF.

Преимущества

- Обеспечивается multiple active connections для каждого контроллера.
- Легко масштабируется для большего числа соединений простым добавлением NIC и алиасов.
- Балансировка нагрузки для контроллеров автоматически обеспечивается политиками Etherchannel IP load balancing policy.

Недостаток

- Не все производители и модели коммутаторов имеют поддержку cross-switch Etherchannel trunks.

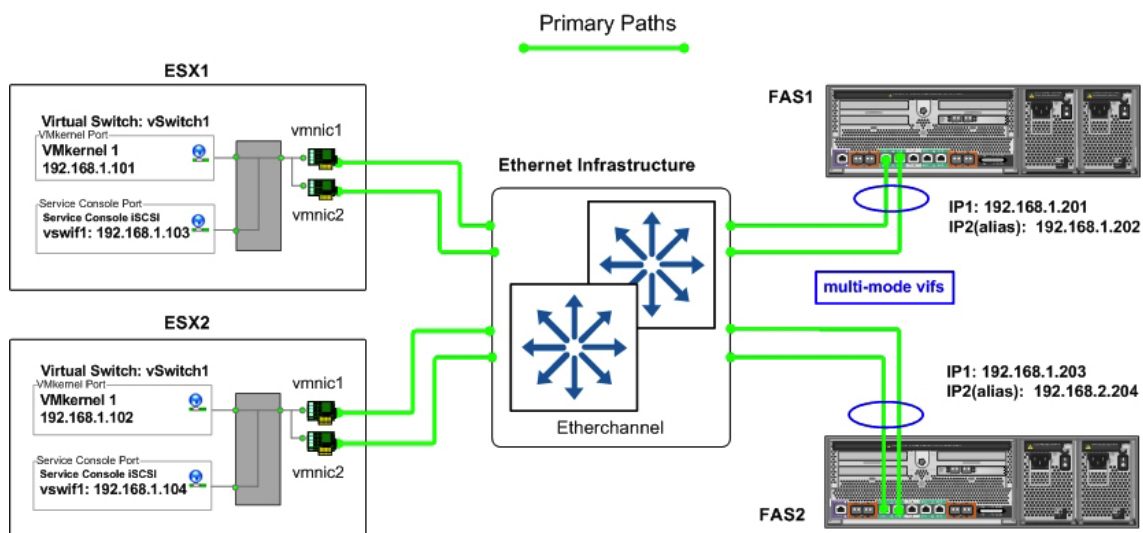


Рис. 35) Использование multimode VIFs совместно с cross-stack Etherchannel.

6.9 КОНФИГУРАЦИЯ DATASTORE С ИСПОЛЬЗОВАНИЕМ ETHERCHANNEL

Дополнительно к правильному конфигурированию vSwitches, сетевых адаптеров, и адресов IP, использование нескольких одновременно работающих физических путей к IP-системе хранения, требует соединения с несколькими датасторами, и задания каждому соединению своего IP-адреса.

Вдобавок к конфигурированию сервера ESX, как показано в примерах, контроллер системы хранения NetApp конфигурируется с IP-адресом в каждой из подсетей, используемой для доступа к датасторам. Это осуществляется с помощью использования объединенных в группы сетевых адаптеров, каждый со своим IP-адресом, или, в некоторых сетевых конфигурациях, назначением алиасов IP-адресов на группу адаптеров, позволяя этим адаптерам работать со всеми необходимыми подсетями

При подключении датастора к серверам ESX, администратор конфигурирует соединение так, чтобы оно использовало один из IP-адресов, назначенных контроллеру системы хранения NetApp. При использовании датастора, подключаемого по NFS, это происходит при задании IP-адреса во время монтирования датастора.

Рисунок ниже показывает схему того, как движется трафик хранения при использовании нескольких серверов ESX и нескольких датасторов.

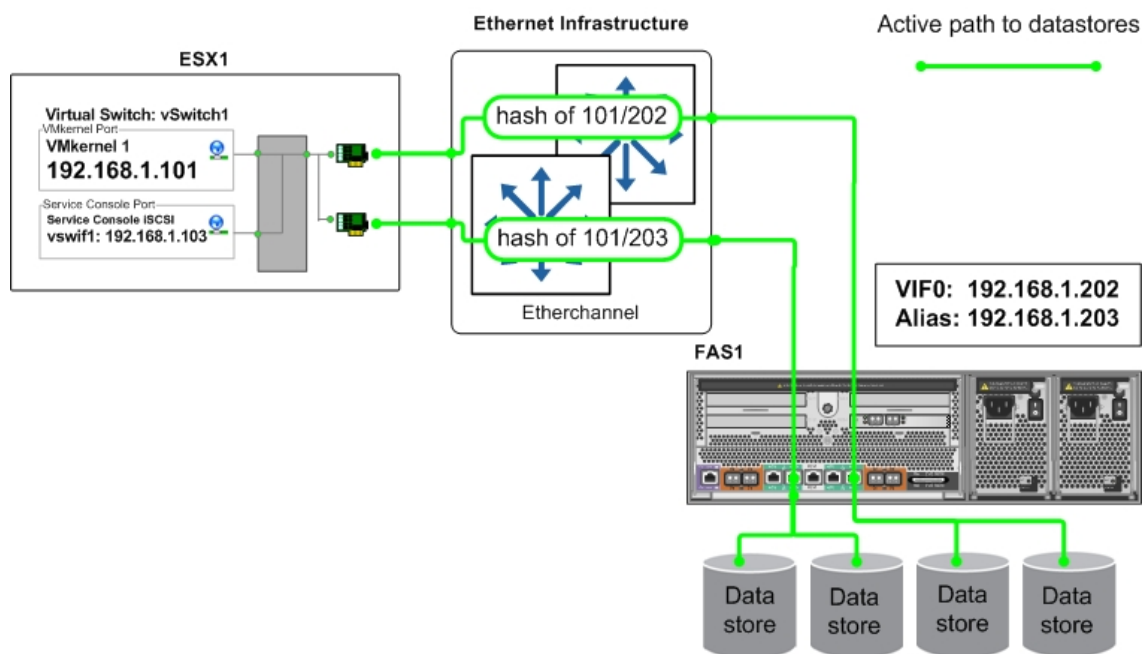


Рис. 36) Подключение датастора с использованием cross-stack Etherchannel.

7. ПУТИ УВЕЛИЧЕНИЯ СТЕПЕНИ ИСПОЛЬЗОВАНИЯ СИСТЕМ ХРАНЕНИЯ

VMware обеспечивает отличные способы увеличить степень использования оборудования физических серверов. При увеличении степени использования оборудования, количество серверного оборудования в датацентре может быть снижено, понижая стоимость владения и стоимость обслуживания датацентра. В типичной системе VMware, процесс миграции физических серверов в виртуальные машины не приводит к уменьшению емкостей распределенных на системах хранения пространств хранения, или количества установленных систем хранения. В обычных случаях, серверная виртуализация никак не влияет на улучшение степени использования систем хранения (а во множестве случаев наблюдается даже обратный эффект).

По умолчанию, в ESX 3.5, виртуальные диски создаются с заполнением всего выделенного им пространства на системе хранения нулями. Этот тип формата VMDK называется «zeroed thick VMDK». VMware предлагает средства использовать меньше места на системе хранения при их создании, с помощью так называемых «thin-provisioned virtual disks». При этом место на хранилище выделяется по мере потребности в нем у VM. Для VMDK, которые созданы на NFS Datastores, формат «thin» предлагается по умолчанию.

«Экономно распределенные» (thin-provisioned) VMDK не доступны для создания в Virtual Infrastructure client в случае использования VMFS Datastores. Чтобы использовать «thin» VMDK на VMFS, вам нужно создать «thin-provisioned» файл VMDK с помощью команды `vmkfstools` с ключом `-d`. Используя технологию VMware thin-provisioning, вы можете снизить количество занятого дискового пространства на VMFS datastore.

VMDK, которые были созданы как диски типа «thin-provisioned», могут быть конвертированы в обычный «thick»-формат, однако вы не можете конвертировать имеющийся диск «thick»-формата в «thin-provisioned», с одним исключением: это возможно, если вы импортируете VMDK формата ESX 2.x в VMDK формата ESX 3.x.

NetApp предлагает технологии виртуализации для систем хранения, которые расширяют возможности, предоставляемые VMware thin provisioning. Дедупликация данных для систем FAS, и методы thin provisioning для VMFS Datastores и RDM LUN-ов предлагают значительные преимущества и экономию, а также существенное увеличение степени использования системы хранения типа NetApp FAS. Обе эти технологии «родные» для систем хранения NetApp, и не требуют каких-то конфигурационных изменений, в случае применения с VMware.

7.1 ДЕДУПЛИКАЦИЯ ДАННЫХ

Одна из наиболее популярных возможностей VMware, это возможность быстро создавать новые виртуальные машины, из «шаблонов» (templates), эталонных инсталляций. VM template включает в себя конфигурационный файл VM (.vmx) а также один или более файлов виртуальных дисков (.vmdk), которые содержат операционную систему, приложения, и необходимые файлы обновлений OS (patch files). Установка из шаблона сберегает время администратора, путем простого копирования конфигурационных файлов и файлов виртуальных дисков и регистрации копии как независимой виртуальной машины. Обычно это процесс включает в себя копирование идентичных данных для каждой новой создаваемой VM. Рисунок 37 показывает пример типичного использования хранилища при установке VI3.

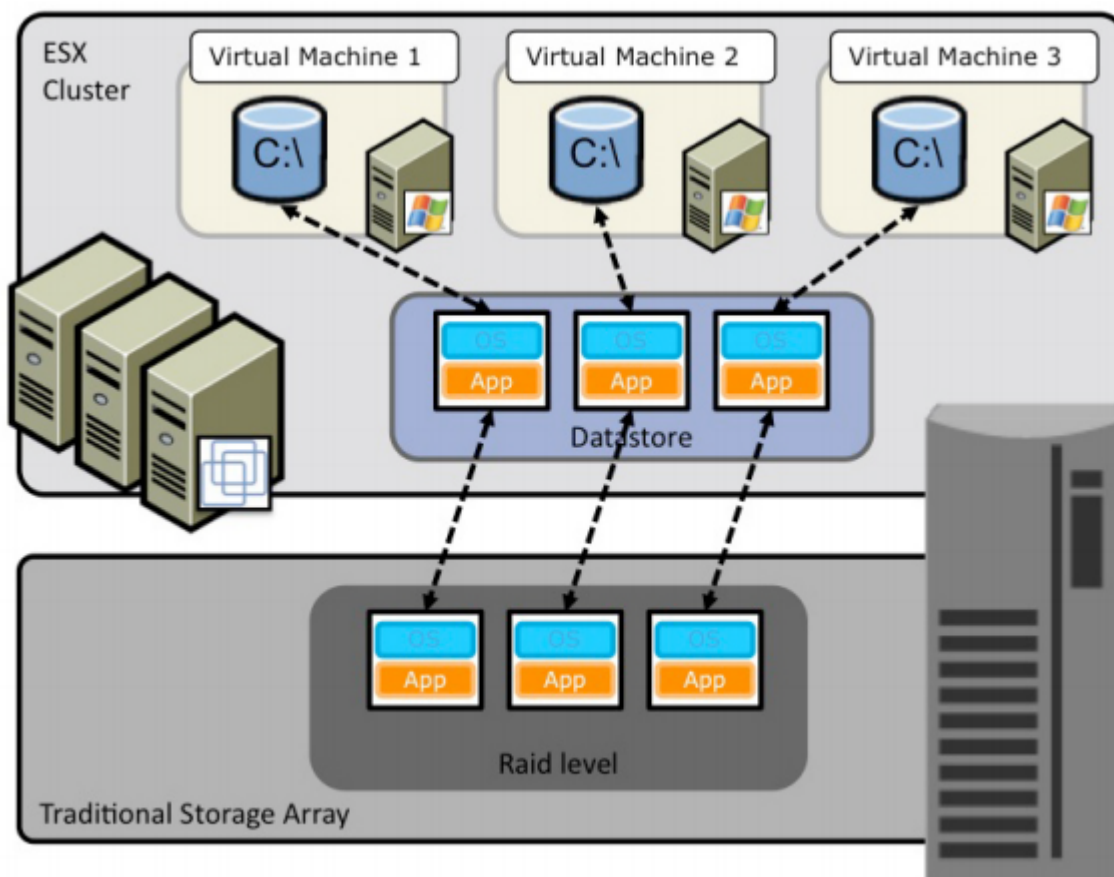


Рис. 37) Использование пространства в традиционной системе хранения.

NetApp предлагает технологию дедупликации данных FAS Deduplication (ранее Advanced Single Instance Storage (A-SIS)). С помощью дедупликации установка VMware может избавиться от дублирующихся во множестве копий блоков данных, значительно увеличивая эффективность использования системы хранения. Дедупликация использует виртуализационную технологию, которая позволяет совместно использовать блоки данных, хранящихся на диске NetApp FAS, несколькими виртуальными машинами, по такому же принципу, как VM совместно используют при работе блоки оперативной памяти. Дедупликация может быть легко внедрена в существующую инфраструктуру, без необходимости менять что-то в существующих практиках администрирования или выполнения задач.

Рисунок 38 показывает пример влияния дедупликации на использование пространства хранения системой VI3.

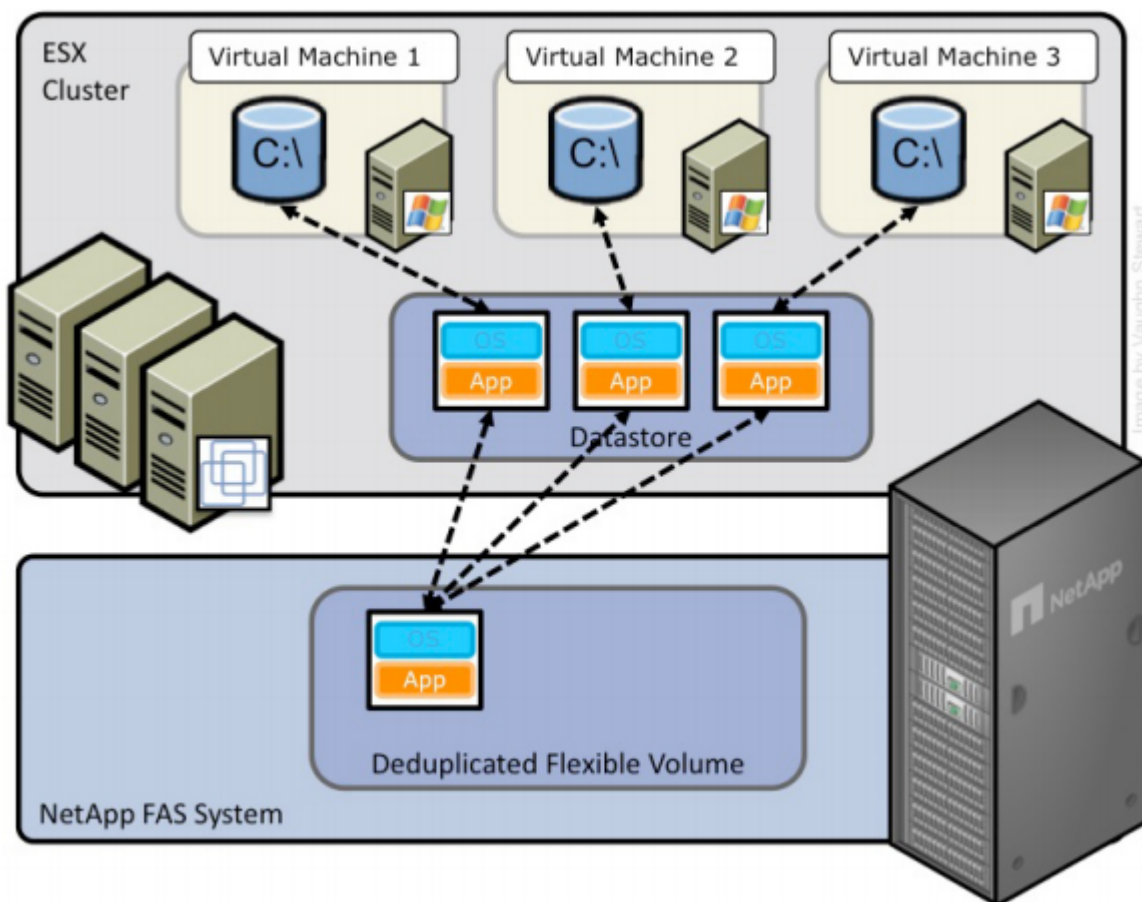


Рис. 38) Использование пространства с использованием дедупликации FAS.

Дедупликация включается на том FAS, и количество высвобожденных в результате дедупликации блоков зависит от характера и повторяемости хранимых на том данных. Для наилучших результатов, NetApp рекомендует группировать сходные операционные системы и сходные приложения в одном datastore, который, в свою очередь, размещается на том с дедупликацией.

Заметьте: Включена ли дедупликация или выключена, это не влияет в плане количества VM, размещаемых на датаstore. Вы должны рассчитывать размер и емкость датаstore такой, какой она должна быть с выключенной дедупликацией.

Дедупликация с VMFS и RDM LUN

Включение дедупликации для созданного LUN создает определенную экономию пространства хранения. Однако при создании LUN с параметрами по умолчанию резервируется на диске пространство для него, равное размеру созданного LUN. Такая модель означает, что хотя система хранения и уменьшает количество физически занятого места, но результат экономии при дедупликации чаще всего оказывается не виден, так как резервирование места, сделанное при создании LUN, не уменьшается.

Чтобы использовать результат экономии места при дедупликации в LUN, вы должны включить для LUN опцию thin provisioning. В подробностях смотрите главу **7.2 Экономное распределение пространства (Thin Provisioning)**, в этом документе. Вдобавок, хотя дедупликация и уменьшает количество использованного пространства, преимущества от этого не видны непосредственно администраторам VMware, так как они видят только уровень LUN, а он, как описывалось в предыдущем абзаце, всегда представляется своим первоначально размеченным размером, вне зависимости от того, сделан ли он традиционным или «thin provisioned».

Дедупликация с NFS

В отличие от описанной выше ситуации с LUN-ами, при использовании дедупликации с NFS, эффект от экономии пространства становится доступным немедленно, и может использоваться администраторами VMware. Никаких дополнительных действий для использования не требуется.

Наилучшие решения по дедупликации, рассматривающие установку расписания ее работы и вопросы производительности можно посмотреть в документе **TR 3505: NetApp A-SIS Deduplication Deployment and Implementation Guide**.

7.2 ЭКОНОМНОЕ РАСПРЕДЕЛЕНИЕ ПРОСТРАНСТВА (THIN PROVISIONING)

Скорее всего, вы хорошо знакомы с традиционными методами распределения пространства на системе хранения, при котором хранилище данных создается и закрепляется непосредственно за конкретным сервером, или, в случае VMware, за виртуальной машиной. Обычная практика администраторов серверов также выделять места для серверов больше реально необходимого, чтобы избежать проблем с внезапным исчерпанием места при работе приложения, а также необходимостью даунтайма приложения при необходимости расширения выделенного ему пространства хранения. Так как никакая система не использует все 100% выделенного пространства хранения, то существует метод виртуализации пространства хранения, позволяющий админам серверов «перерасходовать» пространство хранения, подобно тому, как это делается с серверными ресурсами, такими, как процессор, память и сеть. Такая форма серверной виртуализации называется «экономным распределением пространства» или *thin provisioning*.

Традиционное распределение пространства (*traditional provisioning*) полностью выделяет пространство задаче заранее; экономное распределение (*thin provisioning*) выделяет его по мере потребности в нем у приложения. Ценность «thin-provisioned» хранилища состоит в том, что хранилище при этом работает как единый совместно используемый пул хранения, и место из него потребляется только когда каждая конкретная VM в нем нуждается. Такое совместное использование увеличивает общий уровень использования системы хранения, путем устранения неиспользуемых, но распределенных пространств на нем. Недостаток «экономного распределения пространства» и методики «переиспользования» (*oversubscribing*) состоит в том, что, в том случае, когда каждая VM потребует максимально доступное для нее пространство хранения, мы, без добавления физического пространства дисков, не сможем удовлетворить все эти требования одновременно.

Опции Thin-Provisioning в NetApp

Средства *thin provisioning* у NetApp расширяют возможности *thin provisioning* VMware для VMDK и позволяют сделать, чтобы на LUN-ах, несущих VMFS data store, было занято только столько места, сколько реально записано данных в файлы VMDK (которые, в этом случае, могут быть равно как в «thick», так и в «thin» форме в понимании VMware). Кроме этого LUN-ы подключенные как RDM также могут использовать «thin provisioning». Для создания LUN, использующего *thin provisioning*, сделайте следующее.

1. Откройте FilerView (http://filer/na_admin).
2. Выберите LUN.
3. Выберите Wizard.
4. В окне Wizard нажмите Next.
5. Введите путь.
6. Введите размер LUN.

7. Введите тип LUN (для VMFS выберите VMware; для RDM выберите тип согласно OS вашей VM).
8. Введите описание и нажмите Next.
9. Отключите чекбокс Space-Reserved. См. рис. 39.
10. Нажмите Next и Finish.

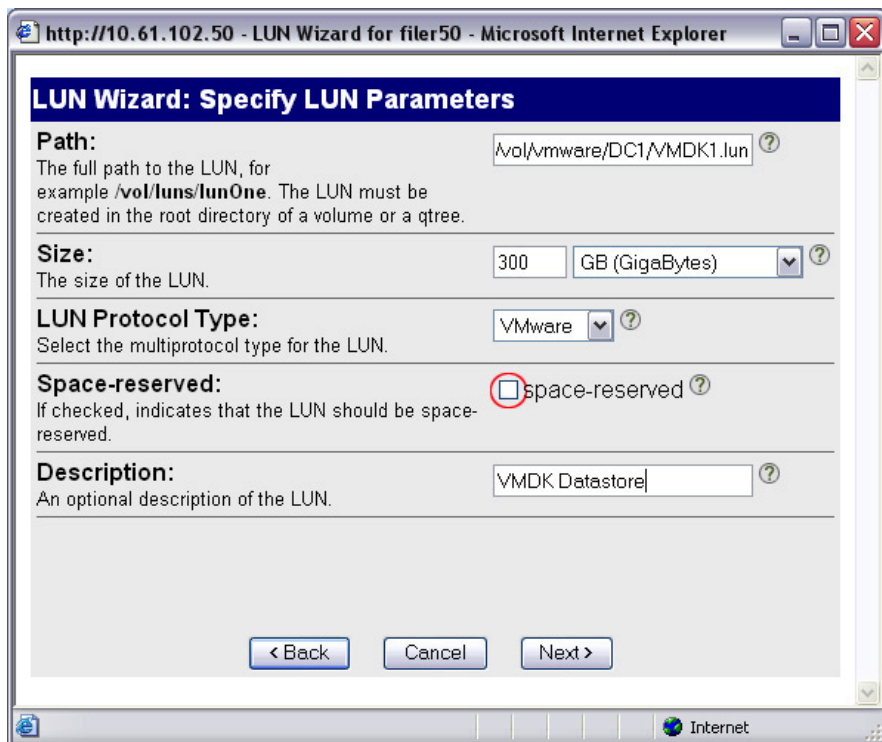


Рис. 39) Включение thin provisioning для LUN.

NetApp рекомендует вам включить и использовать thin provisioning в NetApp, вы также можете сконфигурировать политику управления для тома, содержащего LUN в режиме thin-provisioned. Использование такой политики поможет обеспечить необходимую емкость хранения, когда она понадобится. Политика включает в себя автоматическое изменение размеров тома, автоматическое удаление снэпшотов, и fractional reserve LUN.

Volume Auto Size это опция управления пространством хранения в Data ONTAP, которая позволяет тому расти с определенным шагом увеличения, в случае, если том близок к заполнению. Для системы VMware, NetApp рекомендует устанавливать эту опцию в on. Настройка ее включает в себя определение максимального допустимого размера тома и размер величины прироста.

Для включения этой опции следуйте шагам:

1. Войдите в консоль NetApp.
2. Установите политику volume autosize:
`vol autosize <vol-name> [-m <size>[k|m|g|t]] [-i <size>[k|m|g|t]] on.`

Snapshot Auto Delete это опция политики управления снэпшотами, которая удаляет наиболее старые снэпшоты на томе, когда том близок к заполнению. Для системы VMware, NetApp рекомендует устанавливать порог срабатывания на 5% от доступного места. Дополнительно, вы должны установить опцию тома, чтобы он имел возможность увеличиваться перед тем, как пытаться удалять снэпшоты. Для включения следуйте таким шагам:

1. Войдите в консоль NetApp.

2. Задайте политику snapshot autodelete:
`snap autodelete <vol-name> commitment try trigger volume target_free_space 5 delete_order oldest_first.`
3. Задайте политику volume autogrow:
`vol options <vol-name> try_first volume_grow.`

LUN Fractional Reserve это политика, которая необходима, когда вы используете snapshot-копии тома, содержащего VMware LUN. Эта политика определяет количество дополнительного зарезервированного места, чтобы гарантировать возможность записи в LUN, если том станет заполненным на 100%. Для системы VMware, где используются и Volume Auto Size и Snapshot Auto Delete, и вы используете отдельное пространство для temp, swap, pagefile, и других временных и часто изменяющихся данных из других LUN-ов и томов, NetApp рекомендует устанавливать это значение в 0%. В противном случае оставляйте это значение по умолчанию в 100%. Для установки этой опции сделайте следующее:

1. Войдите в консоль NetApp.
2. Установите volume snapshot fractional reserve:
`vol options <vol-name> fractional_reserve 0.`

8. УПРАВЛЕНИЕ И НАБЛЮДЕНИЕ

8.1 НАБЛЮДЕНИЕ ЗА СИСТЕМОЙ ХРАНЕНИЯ ПРИ ПОМОЩИ NETAPP OPERATIONS MANAGER

NetApp предлагает продукт Operations Manager для наблюдения, управления и создания отчетов по всем системам хранения NetApp FAS в организации. Когда вы используете thin provisioning, NetApp рекомендует установить Operations Manager и настроить уведомление администраторов через e-mail и pager. Для системы хранения, работающей в режиме thin-provisioned очень важно отслеживать расход доступного свободного места.

Правильное и своевременное уведомление об объемах доступного свободного места необходимо для того, чтобы вовремя создавать дополнительное пространство хранения, до того, как оно будет полностью заполнено.

Для подробностей об установке уведомлений с помощью Operations Manger, смотрите:

http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel36r1/html/software/opsmgr/monitor5.htm

http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel36r1/html/software/opsmgr/filesys4.htm

8.2 УПРАВЛЕНИЕ РАСШИРЕНИЕМ ОБЪЕМОВ ХРАНЕНИЯ

Расширение VMFS

Пространство хранения для VMFS может быть довольно просто, однако этот процесс должен быть выполнен только когда виртуальные машины, хранящиеся на datastore, выключены. Для подробностей смотри документ VMware white paper «VMFS Technical Overview and Best Practices.». Для расширения datastore, сделайте следующие шаги:

- 1 Подключитесь к системной консоли FAS (через SSH, Telnet, или кабель консоли).
- 2 Выберите LUN.
- 3 Выберите Manage.
- 4 В левой панели, выберите LUN из списка.
- 5 Введите новый размер LUN в поле Size и нажмите Apply.
- 6 Откройте VirtualCenter.
- 7 Выберите хост ESX.
- 8 Убедитесь, что все виртуальные машины остановлены
- 9 В правой панели выберите закладку Configuration.
- 10 В поле Hardware щелкните Storage Adapters.
- 11 В правой панели выберите HBA и щелкните Rescan.
- 12 В поле Hardware, щелкните Storage.
- 13 В правой панели выделите datastore, который вы хотите увеличить и выберите Properties.
- 14 Щелкните Add Extent
- 15 Выберите LUN и нажмите Next, и после этого снова Next. Пока окно показывает доступное для LUN свободное место, вы можете игнорировать появляющиеся предупреждения (см. рис. 40).
- 16 Убедитесь, что чекбокс Maximize Space установлен, и нажмите Next и Finish.

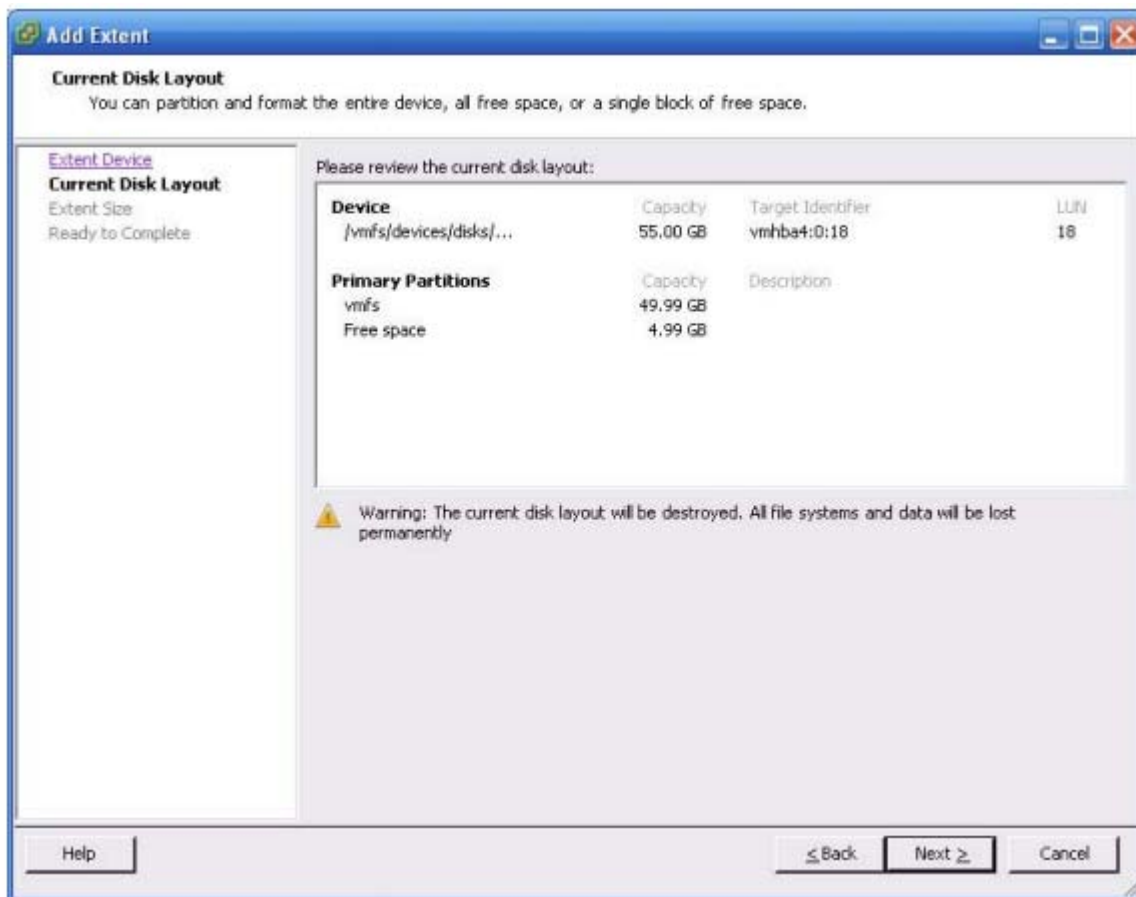


Рис. 40) Расширение раздела VMFS.

Для подробностей о процессе расширения VMFS смотрите **VMware ESX Server 3i Configuration Guide**.

Расширение виртуального диска (VMDK)

Виртуальный диск также может быть расширен; однако этот процесс требует выключения виртуальной машины. Расширение виртуального диска это только половина задачи по расширению доступного пространства; вам также потребуется расширить и файловую систему, после того, как виртуальная машина загрузится. Заметьте, что корневая файловая система, такая как **C: ** в Windows и **/** in Linux не могут быть расширены динамически, когда работает OS. Для расширения этих томов смотрите главу **Расширение загрузочного тома** в этом документе. Для расширения всех прочих томов вы можете использовать собственные средства и инструменты OS. Для расширения виртуального диска следуйте шагам:

1. Откройте Virtual Center.
2. Выберите VM и остановите ее.
3. Щелкните правой клавишей на VM, и выберите Properties.
4. Выберите виртуальный диск, и увеличьте его размер (см. Рис.41)
5. Запустите VM.

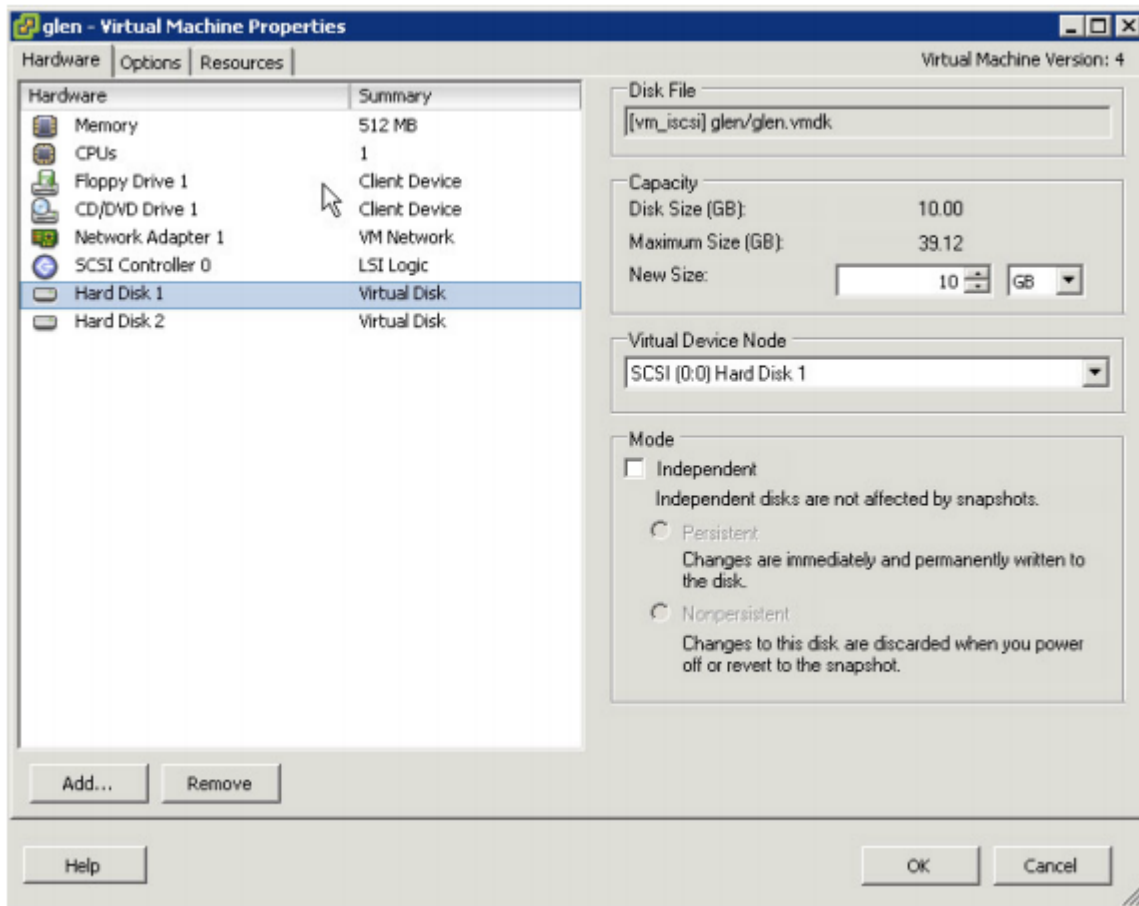


Рис 41) Увеличение размера виртуального диска.

Для подробностей о процессе расширения виртуального диска, смотрите **VMware ESX Server 3i Configuration Guide**.

Расширение Raw Device Mapping (RDM)

Изменение размера при RDM использует частично средства расширения для VMFS и для виртуального диска. Этот процесс требует выключения виртуальной машины. Для расширения хранилища RDM, следуйте таким шагам.

- 1 Откройте VirtualCenter.
- 2 Выберите хост ESX и выключите VM.
- 3 Щелкните правым щелчком на VM и выберите Edit Settings, чтобы открыть окно Edit Settings.
- 4 Выделите жесткий диск, который будет изменяться и нажмите Remove. Выберите радиокнопку Remove from Virtual Machine и выберите Delete Files from Disk. Это действие удалит Mapping File, но НЕ удалит данные с RDM LUN. См. рис. 42.
- 5 Откройте FilerView (http://filer/na_admin).
- 6 Выберите LUN.
- 7 Выберите Manage.
- 8 Из списка в левой панели выберите LUN.
- 9 В поле Size, введите новый размер LUN и щелкните Apply.
- 10 Откройте VirtualCenter.
- 11 В правой панели выберите закладку Configuration.

- 12 В поле Hardware выберите Storage Adapters.
- 13 В правой панели выберите HBA и щелкните Rescan.
- 14 Щелкните правой клавишей на VM и выберите Edit Settings, чтобы открыть окно Edit Settings,
- 15 Нажмите Add, и выберите Hard Disk, затем Next. См. рис. 43.
- 16 Выберите LUN и нажмите Next. См. рис. 44.
- 17 Определите VMFS datastore, который будет содержать Mapping File.
- 18 Запустите VM. Помните, что после того, как вы увеличили LUN, вам нужно также увеличить файловую систему на нем. Следуйте указаниям главы **Расширение файловой системы VM** ниже.

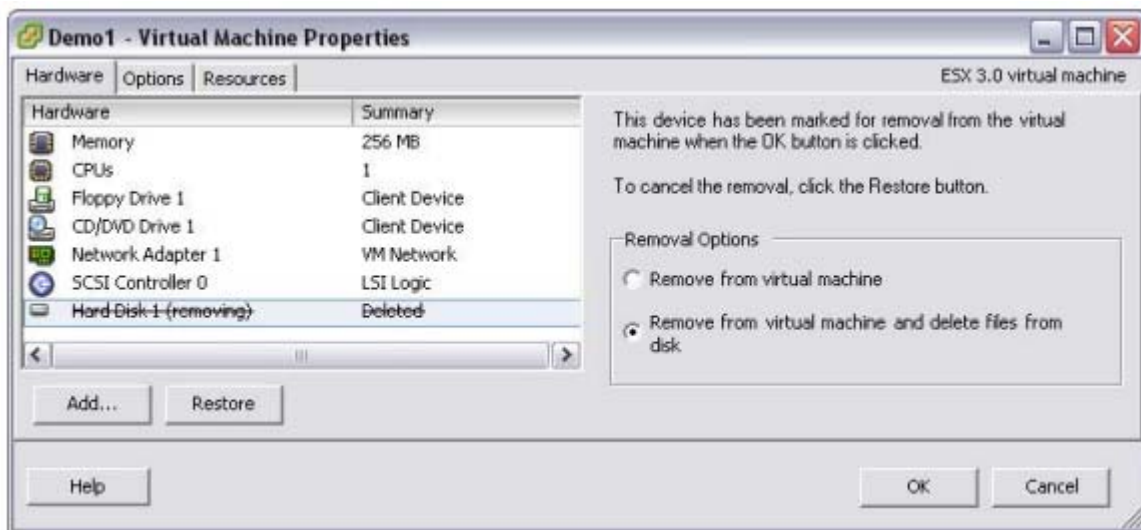


Рис. 42) Удаление VMDK из VM.



Рис. 43) Подключение RDM к VM.

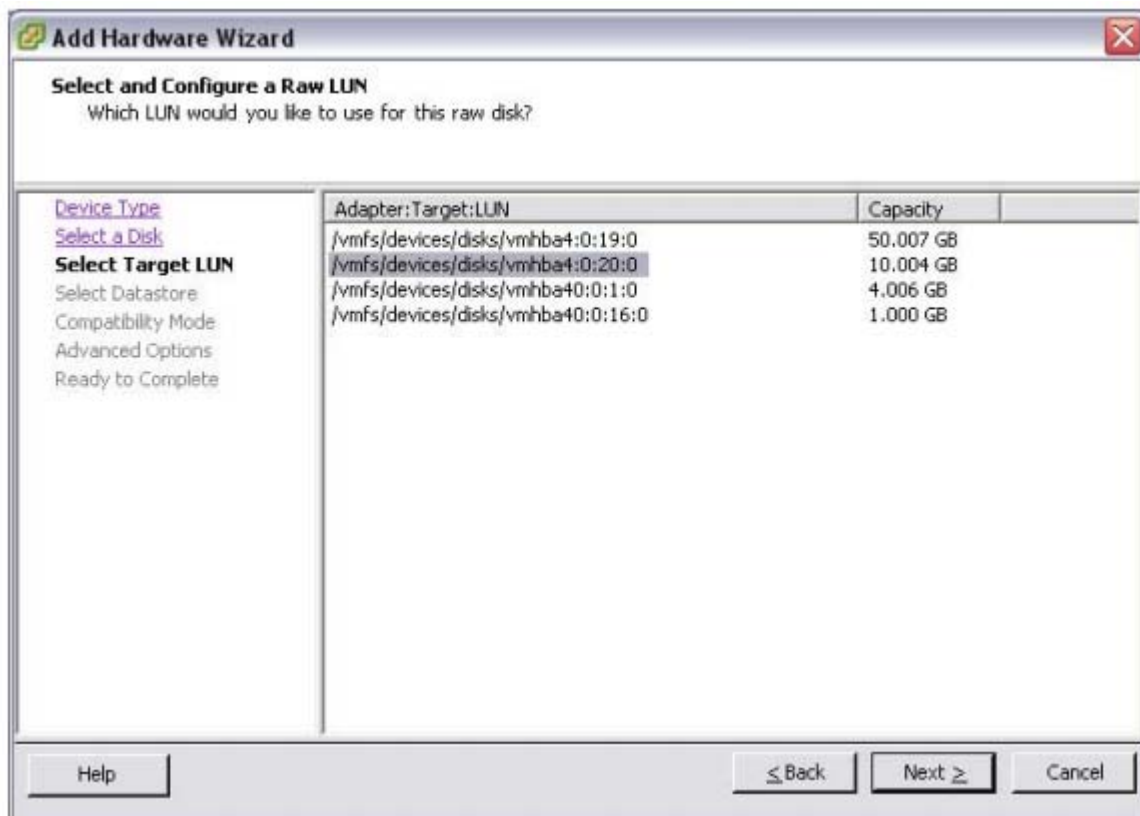


Рис. 44) Выбор LUN для монтирования в качестве RDM.

Расширение файловой системы VM (NTFS или EXT3)

Когда виртуальный диск или RDM увеличивает свой размер, вам также нужно расширить файловую систему, находящуюся на нем. Этот процесс может быть сделан «на ходу», с запущенной VM, используя собственные инструменты системы, или свободно распространяемые программы.

1. Подключитесь к VM
2. Расширьте файловую систему
3. Для Windows VM, для того, чтобы увеличить файловую систему, вы можете воспользоваться утилитой diskpart. Для подробностей смотрите статью <http://support.microsoft.com/default.aspx?scid=kb;en-us;300415>.

Для Linux VM, для увеличения файловой системы, вы можете воспользоваться утилитой ext2resize. Для подробностей смотрите <http://sourceforge.net/projects/ext2resize>.

Расширение загрузочного тома с гостевой OS

Корневой, том, такой как C: \ в Windows VM и / в Linux VM не может быть увеличен «на лету», или пока система используется. Есть простой способ расширить эту файловую систему, которая не требует для этого приобретения дополнительных программ (исключая ext2resize). Для этого способа нужно, чтобы VMDK или LUN которые должны быть расширены, были подключены к другой виртуальной машине, с такой же OS, используя процесс, описанный ранее. Когда диск подключен, то эта VM может запустить инструмент расширения файловой системы. После расширения файловой системы, эта VM выключается, и диск отсоединяется. После переподключения диска к исходной VM и ее загрузки, вы можете увидеть, что загрузочная партиция имеет новый размер.

9. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

9.1 ТЕХНОЛОГИИ SNAPSHOT

В VMware Virtual Infrastructure 3.0 появилась возможность создавать снэпшот-копии виртуальных машин. Технология снэпшотов использует создание «point-in-time» копий, обеспечивающих быстрое восстановление VM в предшествующее их состояние, на момент создания снэпшота. Компания NetApp с 1992 года предоставляет возможность пользователям создавать и использовать снэпшоты на своих системах, и, хотя базовая концепция снэпшотов сходна и у NetApp и у VMware, вы должны понимать важную разницу между ними, и моменты, когда вы должны предпочесть тот или другой вариант.

Снэпшоты VMware создают простую point-in-time версию виртуальной машины, позволяющую осуществить быстрый откат ее состояния на нужный момент времени. Преимущества снэпшотов VMware в том, что их легко создать и использовать, так как они создаются непосредственно из VirtualCenter. VMware считает, что их технология снэпшотов в ESX не предназначена для резервного копирования Virtual Infrastructure. Для подробностей о собственных снэпшотах VMware, включая руководство по их использованию, смотрите **VMware Basic System Administration Guide** и **VMware Storage/SAN Compatibility Guide for ESX Server 3.5 and ESX Server 3i**.

Технология NetApp Snapshot может быть легко интегрирована в инфраструктуру VMware, обеспечивая так называемую «crash-consistent» версию виртуальных машин для целей восстановления VM, их клонирования, репликации и катастрофоустойчивости. Преимуществом такого решения является то, что это единственная на рынке технология снэпшотов, которая не приводит к снижению производительности системы хранения при ее использовании. Сам VMware считает, что для оптимальной производительности и масштабируемости, аппаратные снэпшоты предпочтительнее программных. Недостаток решения заключается в том, что оно не управляется из VirtualCenter, требует внешних скриптов и/или расписания выполнения для управления процессом их создания. Для подробностей смотрите **VMware Basic Systems Administration Guide** и **VMware ESX Server 3i Configuration Guide**.

9.2 РАЗМЕЩЕНИЕ ДАННЫХ ДЛЯ SNAPSHOT-КОПИИ

Когда вы используете NetApp Snapshot-копии, или SnapMirror, то NetApp рекомендует отделять незначимые и временные данные с того виртуального диска, что будет копироваться в снэпшот или реплицироваться с помощью SnapMirror. Так как Snapshot-копии NetApp удерживают за собой блоки с данными, которые не могут использоваться, пока не удален использующий их снэпшот, временные, незначимые и часто изменяющиеся данные займут неоправданно большое количество места за короткое время. Вдобавок, если вы реплицируете вашу систему с целью обеспечения непрерывности бизнеса или резервного копирования disk-to-disk, ошибка в отделении важных данных от незначимых будет означать значительное увеличение объемов репликации, трафика передачи данных, и времени, уходящего на каждый цикл репликации.

Виртуальные машины должны размещать свои swap-файлы, pagefile, пользовательские и системные директории временных файлов, на отдельных виртуальных дисках, размещенных на отдельном датасторе, выделенном на NetApp FAS под такого рода данные. Вдобавок к этому сам сервер ESX создает swap-файл VMware для каждой запущенной VM. Эти файлы также должны быть перемещены на отдельный датастор, помещенный на отдельный том NetApp. Рисунок 45 показывает пример такого размещения данных при конфигурировании VM.

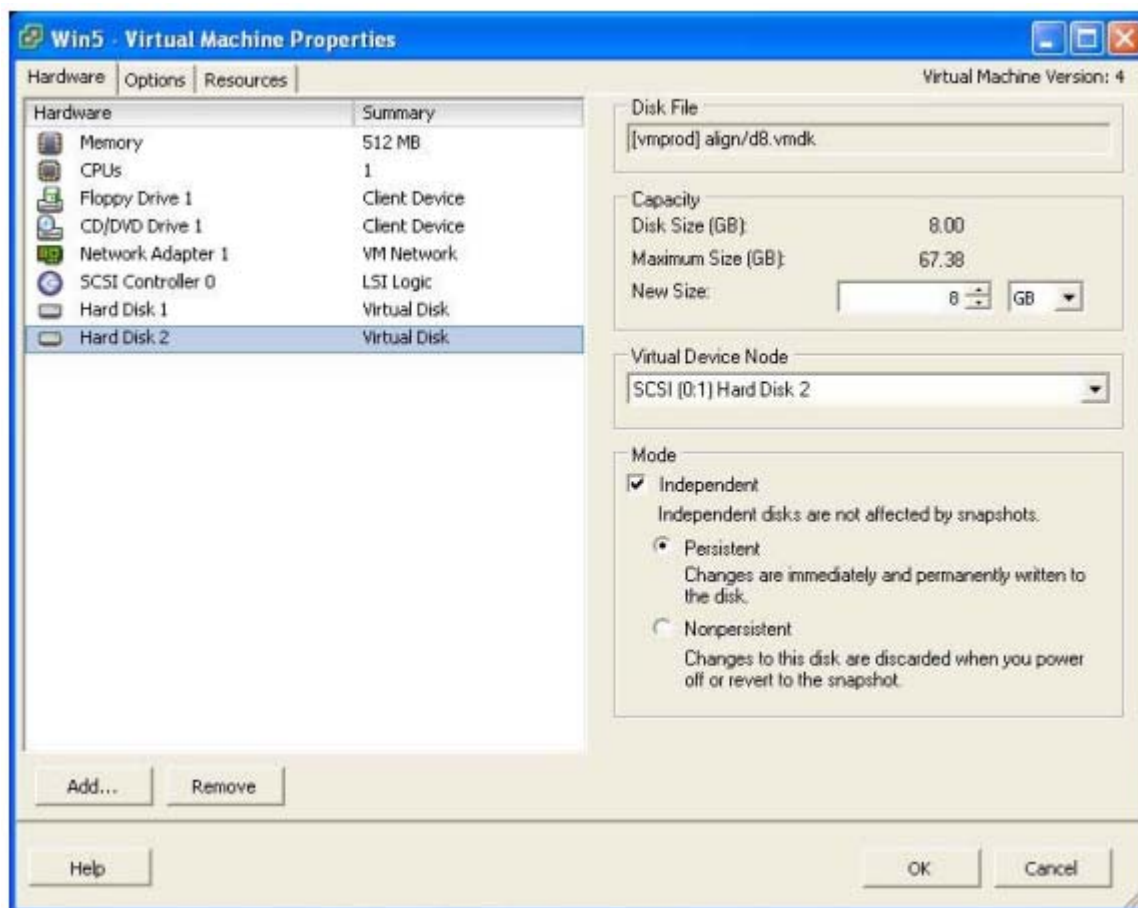


Рис. 45) Конфигурирование независимого диска.

Например, если у вас есть группа виртуальных машин, которые создают Snapshot-копии три раза в день, и одна, создающая их раз в день, то вам нужно создать для них как минимум четыре тома NetApp (том рабочих данных первой группы, том под swap, temp и логи первой группы, и так же для второй). Для традиционных виртуальных дисков, размещенных на VMFS, каждый том содержит один LUN; для виртуальных дисков, размещенных на NFS, каждый том содержит несколько файлов виртуальных дисков; в случае RDM, каждый том содержит несколько RDM-форматированных LUN-ов. Скрипт для Snapshot-бэкапа должен быть сконфигурирован для каждого тома, содержащего VM, и иметь соответствующее требованиям расписание работы.

Размещение данных виртуальных машин

Этот раздел рассматривает вопросы размещения на дисках временных данных, являющихся частью виртуальной машины. Примеры рассматривают в качестве гостевой OS систему Windows, так как установка необходимой схемы размещения файлов данных для нее несколько сложнее, чем для других OS; однако те же принципы применимы и для других операционных систем. Чтобы снизить затраты времени на создание правильной конфигурации, вам нужно сделать эталонный «виртуальный диск» с нужной файловой системой, и клонировать его средствами VMware, когда вам понадобится создать новую виртуальную машину.

Приведенный ниже файл реестра это пример простой установки места расположения файла подкачки (pagefile) и места хранения временных файлов (temp area) (как для пользовательских данных, так и для OS) на диск D: \. Этот файл должен быть импортирован в реестр сразу, как только создана виртуальная машина. Если диск D: \ не существует, то будут использованы системные значения по умолчанию. Процесс внедрения этого файла в реестр может быть автоматизирован с помощью Microsoft Setup Manager. Чтобы использовать эти значения, скопируйте содержимое примера в файл и запишите его как текстовый файл под

именем temp.reg. В Microsoft Setup Manager есть раздел, где вы можете добавить ваш temp.reg для импорта в реестр, при первом запуске виртуальной машины. Для подробностей по автоматизации процесса развертывания клонированных серверов Windows, смотри руководство по Microsoft Setup Manager.

Registry file example script:

Start-----

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\Session Manager\Memory Management]
```

```
"PagingFiles"=hex(7):64,00,3a,00,5c,00,70,00,61,00,67,00,65,00,66,00,69,00,6c,
```

```
\
```

```
00,65,00,2e,00,73,00,79,00,73,00,20,00,32,00,30,00,34,00,38,00,20,00,32,00,
```

```
\
```

```
30,00,34,00,38,00,00,00,00,00
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\Session Manager\Environment]
```

```
"TEMP"="D:\  
\"
```

```
"TMP"="D:\  
\"
```

```
[HKEY_CURRENT_USER\Environment]
```

```
"TEMP"="D:\  
\"
```

```
"TMP"="D:\  
\"
```

```
[HKEY_USERS\.DEFAULT\Environment]
```

```
"TEMP"="D:\  
\"
```

```
"TMP"="D:\  
\"
```

End -----

Размещение VMware Swap и Log File

VMware ESX Server создает swap-файл и log-и для каждой запущенной VM. Размер этих файлов изменяется динамически в соответствии с разницей между объемом физической памяти на сервере и количеством памяти, выделенной данной виртуальной машине.

Так как эти данные по природе постоянно изменяющиеся, то, если мы хотим использовать технологию NetApp Snapshot, они должны быть отделены от наших данных собственно виртуальной машины.

Рис. 46 показывает пример такой схемы размещения данных.

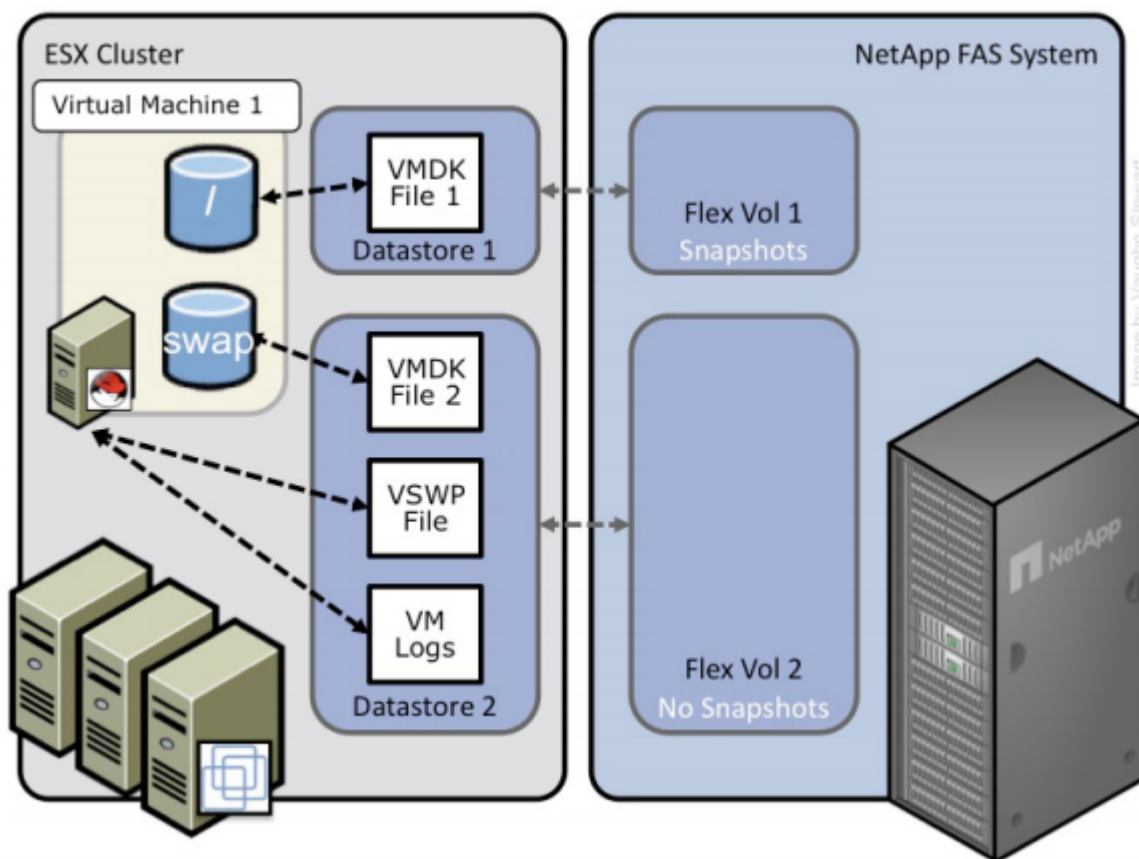


Рис. 46) Оптимизированная схема размещения данных для использования NetApp Snapshots

.Предварительно нам надо создать VMFS или NFS datastore для хранения swap-файлов. Так как swap-файл в VMware динамический по природе, то NetApp рекомендует создать достаточно большой «thin-provisioned» LUN или FlexVol с включенной опцией «auto grow». Как «thin-provisioned» LUN, так и FlexVol с опцией «auto grow» предлагают значительное преимущество при хранении swap-файлов. При такой схеме не требуется управление выделением пространства под swap и не снижается степень эффективности использования системы хранения. В сравнении с традиционными методами хранения swap-файла VMware, такая схема имеет преимущества, так как иначе, если вы выделите недостаточно места, то VM не запустится, а если места под хранение swap выделено чрезмерно, то вы теряете слишком много выделенного но неиспользуемого места.

Для конфигурирования этих настроек следуйте таким шагам (и смотрите Рис.47):

1. Откройте VirtualCenter.
2. Выберите сервер ESX.
3. В правой панели выберите закладку Configuration.
4. В блоке Software, выберите Virtual Machine Swap Location.
5. В правой панели выберите Edit.
6. Откроется Virtual Machine Swapfile Wizard
7. Выберите datastore, которая будет глобальным местом размещения.
8. Повторите шаги от 2 до 7 для каждого ESX в кластере
9. Существующие VM должны быть перезапущены для перемещения VSwap

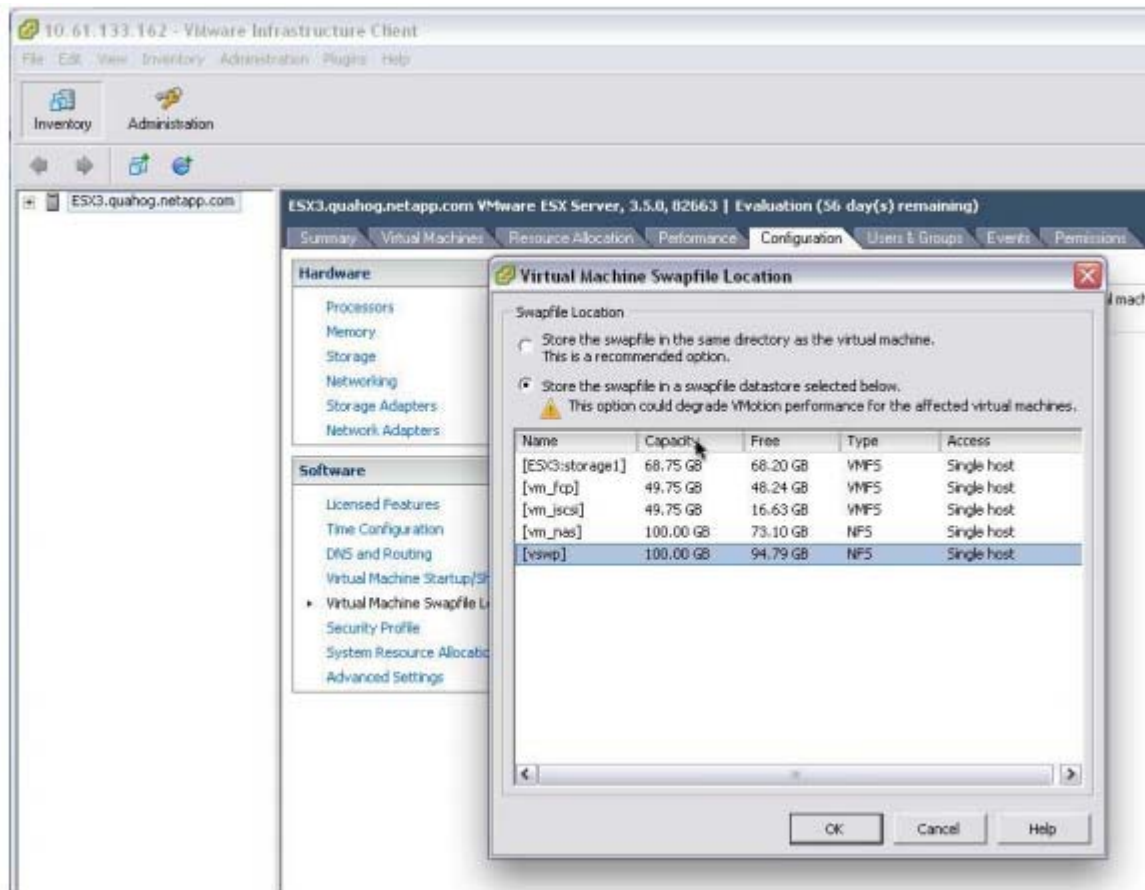


Рис. 47) Конфигурирование размещения виртуальных swar-файлов

Для конфигурирования датастора, под размещение виртуальных swar-файлов развернутых VM, сделайте следующее:

(см. Рис. 48).

1. Откройте VirtualCenter.
2. Выберите виртуальную машину или шаблон VM.
3. Если виртуальная машина работает – выключите ее и удалите из inventory.
4. Подключитесь к консоли ESX (через ssh, telnet или консольное подключение).
5. Выберите vmx, который будете редактировать.
6. Добавьте строку `workingDir = /vmfs/volumes/<volume_name_of_temp>`.
7. Добавьте виртуальную машину назад в inventory (не нужно, если это был шаблон)
8. Повторите описанные пункты от 2 до 7 для всех необходимых вам VM.

VMware документировал, что следующие опции **не должны** присутствовать в файле VMX, при использовании глобального размещения VSwar:

`sched.swap.dir`

`sched.swap.derivedName`

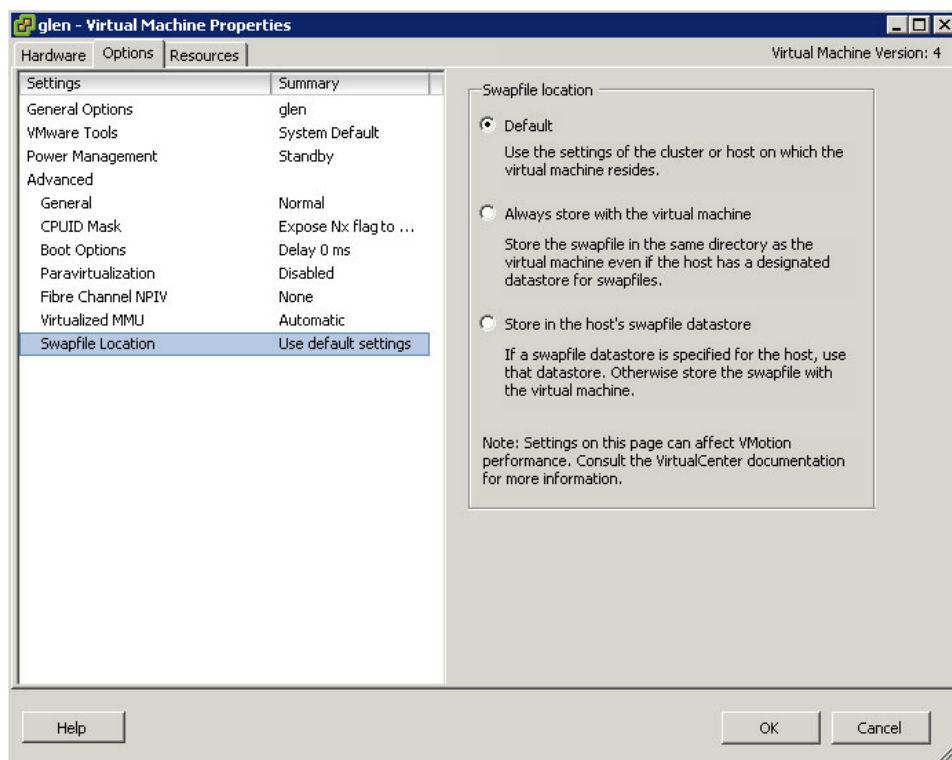


Рис 48) Проверка размещения виртуальных swap-файлов в VM.

10. РЕЗЕРВНОЕ КОПИРОВАНИЕ ПРИ ПОМОЩИ SNAPSHOTS В VMWARE

10.1 ИСПОЛЬЗОВАНИЕ NETAPP SNAPSHOT BACKUP ДЛЯ VMWARE VIRTUAL INFRASTRUCTURE

Возможность быстро создавать резервные копии десятков виртуальных машин, без снижения производительности системы в целом, может помочь и ускорить переход компании в виртуальную серверную инфраструктуру. NetApp предлагает использовать для этого SnapManager for Virtual Infrastructure (SMVI). SMVI создан в рамках общего портфолио продуктов NetApp SnapManager, обеспечивая дисковую резервную копию, хранящую только измененные блоки каждой виртуальной машины, и может обеспечить множественные точки восстановления информации на протяжении всего рабочего дня, а так как средство резервного копирования это интегрированный компонент системы хранения, то SMVI обеспечивает время восстановления меньшее, чем любое другое средство.

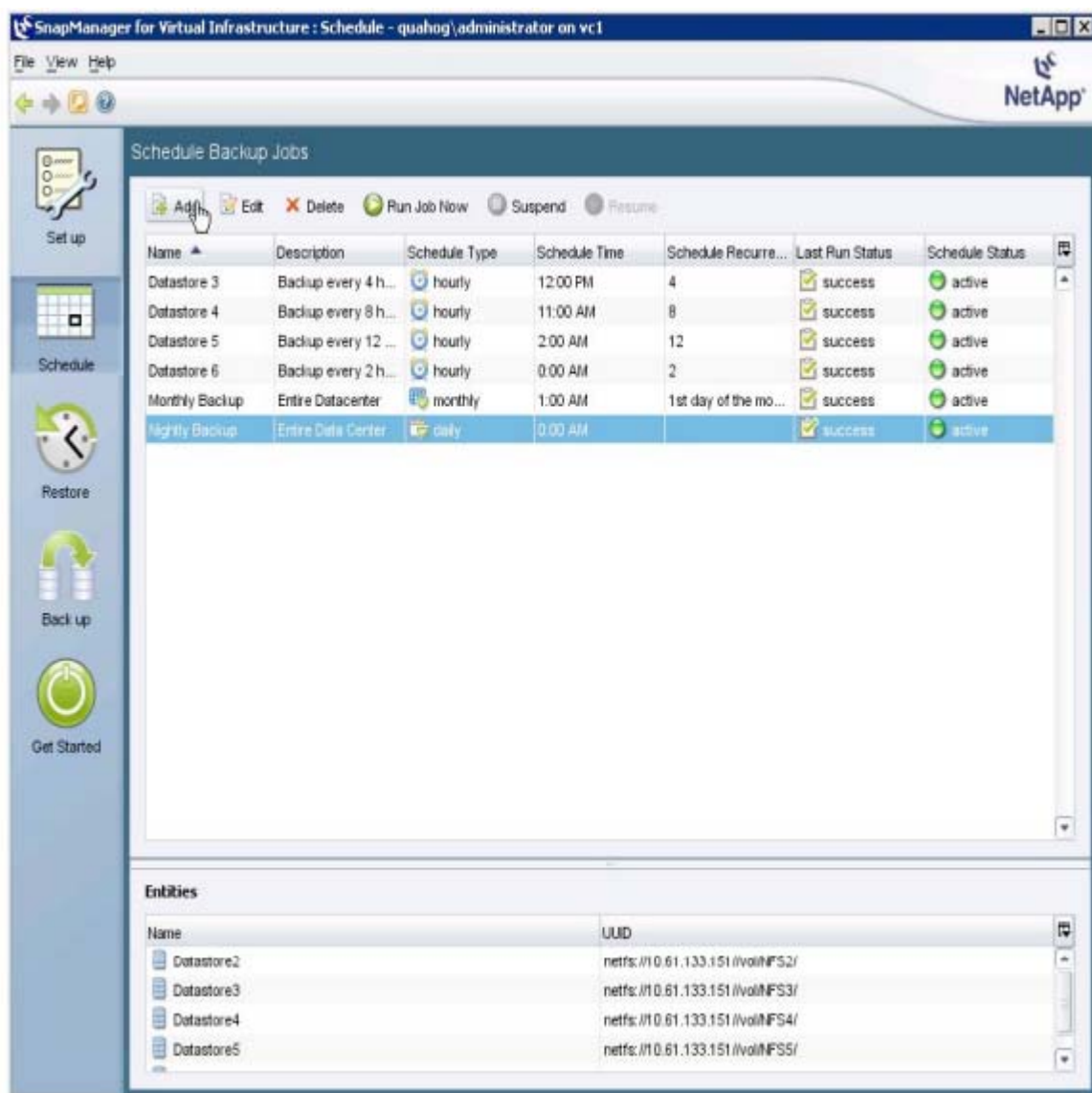


Рис. 49) Установка политик резервного копирования для datastore в SnapManager for Virtual Infrastructure.

Для подробностей о SnapManager for Virtual Infrastructures смотрите NetApp technical Library.

Если вы хотите использовать резервное копирование и восстановление управляемое скриптом, то смотрите Приложение 1 в этом документе.

11. ВЫВОДЫ

VMware Virtual Infrastructure предлагает пользователям несколько методов использования системы хранения с виртуальными машинами. Каждый из этих методов предлагает пользователю гибкие возможности для построения его инфраструктурного решения, экономии средств, увеличения степени использования ресурсов хранения, усиления степени защиты данных и скорости их восстановления.

Этот технический документ не является исчерпывающим руководством по установке или созданию решения. Для конкретного решения может потребоваться провести определенный экспертный анализ. В случае необходимости поговорите с вашим контактом в NetApp, чтобы связаться с нашими экспертами по решениям VMware.

Замечания по содержанию этого документа с удовольствием будут приняты авторами.

12. ПРИЛОЖЕНИЕ 1: КОНФИГУРИРОВАНИЕ СИСТЕМЫ ДЛЯ ВЫПОЛНЕНИЯ СКРИПТА РЕЗЕРВНОГО КОПИРОВАНИЯ В SNAPSHOT

12.1 КОНФИГУРАЦИЯ ESX ДЛЯ ИСПОЛЬЗОВАНИЯ SNAPSHOT-КОПИЙ

В системе VMware Virtual Infrastructure, пространство хранения, выделенное виртуальным машинам, хранится в файлах виртуальных дисков (расположенных на VMFS или NFS) или на смонтированных в VM «физических» LUN без файловой системы (raw device mapping, RDM). Администраторы VI3 могут монтировать созданные системой хранения snapshot-копии VMFS LUN-ов. С помощью этой возможности, пользователи могут подключать snapshot-копии как VMFS так и RDM LUN-ов на сервере ESX. Для использования этой функциональности следуйте шагам:

- 1 Откройте VirtualCenter.
- 2 Выберите ESX Server.
- 3 В правой панели выберите закладку Configuration.
- 4 В поле Software, выберите Advanced Settings и откройте окно Advanced Settings.
- 5 В левой панели выберите LVM.
- 6 В правой панели введите значение 1 в поле LVM. EnableResignature box.
- 7 Повторите шаги с 2 по 6 для каждого вашего ESX Server.

12.2 КОНФИГУРИРОВАНИЕ SSH ДЛЯ ИСПОЛЬЗОВАНИЯ С ESX SERVER И NETAPP FAS

Наиболее эффективный способ интегрировать Snapshot-копии NetApp, это организовать централизованное управление и выполнение команд создания снэпшотов. NetApp рекомендует сконфигурировать систему хранения FAS и сервера ESX, разрешив одному хосту удаленно выполнять команды на обеих системах. Этот администраторский хост должен иметь установленный и настроенный SSH-клиент.

Конфигурация системы хранения FAS для использования SSH

Для того, чтобы сконфигурировать доступ по SSH к системе хранения NetApp FAS, сделайте следующее:

- 1 Подключитесь к системной консоли FAS (через SSH, Telnet, или консольный кабель).
- 2 Выполните следующие команды:

```
secureadmin setup ssh
options ssh.enable on
options ssh2.enable on
```
- 3 Войдите как root на систему Linux или VMware, которые будут выполнять удаленные команды FAS.
- 4 Добавьте Triple DES в список доступных SSH-ciphers; это единственный cipher, с которым работает NetApp FAS. Отредактируйте файл /etc/ssh/sshd-config и исправьте строку «Ciphers» так как показано:

```
Ciphers aes128-cbc, aes256-cbc, 3des-cbc.
```
- 5 Сгенерируйте DSA host key. На Linux или VMware ESX Server, используйте следующую команду:

```
ssh-keygen -t dsa -b 1024.
```

Когда будет запрошена passphrase, не вводите ничего; вместо этого нажмите Enter. Public key будет записан в /root/.ssh/id_dsa.pub.

- 6 Смонтируйте корневую файловую систему FAS как root
- 7 Скопируйте информацию ключа из файла public key в систему хранения FAS /etc/ssh/root/.ssh/authorized_keys, удалив всю информацию, исключая то, что находится до строки ssh-dsa и строки комментария. Смотри пример ниже.
- 8 Проверьте подключение от удаленного хоста, выполнив команду version на системе FAS. Это не должно спрашивать пароля.
ssh <netapp> version
NetApp Release 7.2: Mon Jul 31 15:51:19 PDT 2006

Это пример ключа для хоста:

```
ssh-dsa  
AAAAB3NzaC1kc3MAAABhALVbwVyhtAVoaZukcj STI Rb/RE01/ywbQECtAchi j zdzhEJUz9Qh96HVEwyZ  
Ddah+PTxfyi tJCerb+1FAn065v4WMq6j xPVYto6l 5l b5zxfg2l /hhT/6KPzi S3LTZj KccwAAABUAj kLM  
wkpi Pmg8Unv4fj CsYYhrSLOAAABgF9NsuZxni 00Hnr8tmW5RMX+M6VaH/nl JUzVXbLi l 8+pyCXALQ29Y  
31uV3SzWtd1V0gj JHgv0GBw8N+rvGSB1r60VqggGj SB+ZXA01Eecbnj vLnUtF0TVQ75D9auagj OAAAA  
YEJPx8wi 9/CaS3dfKJR/tYy7Ja+MrI D/RC0gr22XQP1ydexsFYQxenxzExPa/sPj A45YtcUom+3mi eF  
aQuWHZSNFr8sVJoW3LcF5g/z9Wkf5GwvGGtD/yb6bcsj Z4tj l w==
```

Конфигурирование SSH для использования с ESX

Чтобы сконфигурировать ESX Server для приема соединений с использованием SSH, следуйте этим шагам:

- 1 Войдите на консоли ESX как root.
- 2 Включите сервисы SSH с помощью следующих команд:
esxcfg-firewall -e sshServer
esxcfg-firewall -e sshClient
- 3 Перейдите в папку конфигурации SSH-сервера:
cd /etc/ssh.
- 4 Отредактируйте конфигурационный файл:
vi sshd_config
- 5 Измените следующую строку:
PermitRootLogin no
на:
PermitRootLogin yes
- 6 Перезапустите сервис SSH с помощью команды:
service sshd restart
- 7 Создайте SSH public key:
ssh-keygen -t dsa
эта команда выведет содержимое, похожее на приведенный ниже пример. Сохраните его в место по умолчанию и не вводите passphrase.
- 8 Перейдите в папку .ssh:
cd /root/.ssh
- 9 Запустите следующую команду:
cat id_dsa.pub >> authorized_keys
chmod 600 authorized_keys
- 10 Повторите шаги с 1 по 9 для каждого вашего ESX Server.

Пример вывода:

```
Generating public/private dsa key pair.  
Enter file in which to save the key (/home/root/.ssh/id_dsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/root/.ssh/id_dsa.  
Your public key has been saved in /home/root/.ssh/id_dsa.pub.  
The key fingerprint is:  
7b:ab:75:32:9e:b6:6c:4b:29:dc:2a:2b:8c:2f:4e:37 root@hostname  
Your keys are stored in /root/.ssh.
```

12.3 ВОССТАНОВЛЕНИЕ ВИРТУАЛЬНОЙ МАШИНЫ ИЗ SNAPSHOT-КОПИИ VMFS

Использование Snapshot-копии датастора VMFS предлагает быстрый метод восстановления VM. В целом этот процесс осуществляет выключение VM, подключение к Snapshot-копии VMFS LUN, копирование VMDK из Snapshot-копии в действующую VMFS, и включение VM. Для совершения такого процесса выполните следующие шаги.

- 1 Откройте VirtualCenter.
- 2 Выберите хост ESX и выключите VM.
- 3 Войдите на консоли ESX как root.
- 4 Переименуйте файлы VMDK:
`mv <current VMDK path> <renamed VMDK path>`
- 5 Подключитесь к системной консоли FAS (через SSH, Telnet, или консольный кабель).
- 6 Клонировать исходный LUN из недавней Snapshot-копии, переведите его в онлайн и замапьте его. На консоли системы хранения выполните:
`lun clone create <original LUN path> -b <original LUN path>
<Snapshot name>
lun online <LUN path>
lun map <LUN path> <igroup> <ID>`
- 7 Откройте VirtualCenter.
- 8 Выберите хост ESX.
- 9 На правой панели выберите закладку Configuration.
- 10 В поле Hardware, выберите линк Storage Adapters.
- 11 В верхнем правом углу, выберите линк Rescan. Сканируйте новый раздел и VMFS datastores. На VMFS datastore появятся Snapshot-ы.
- 12 Войдите на консоли ESX как root.
- 13 Скопируйте виртуальные диски из папки Snapshot datastore в рабочую VMFS:
`cd <VMDK snapshot path>
cp <VMDK> <production VMDK path>`
- 14 Откройте VirtualCenter.
- 15 Выберите хост ESX и включите VM.

- 16 Убедитесь, что вы восстановили правильную версию. Залогиньтесь в VM и проверьте, что система восстановлена в нужном вам состоянии, на нужный момент времени.
- 17 Подключитесь к системной консоли FAS (через SSH, Telnet, или консольный кабель).
- 18 Удалите Snapshot-копию LUN:
`lun destroy -f <LUN path>`
- 19 В верхнем правом углу щелкните Rescan. Просканируйте как новое хранилище, так и VMFS datastore.

12.4 ВОССТАНОВЛЕНИЕ ВИРТУАЛЬНОЙ МАШИНЫ ИЗ SNAPSHOT-КОПИИ NFS

NFS предлагает быстрый метод восстановления VM из Snapshot-копии. Вкратце, это процесс выключения VM, восстановления VMDK, и включения VM. Чтобы выполнить эти шаги следуйте таким шагам.

- 1 Откройте VirtualCenter.
- 2 Выберите хост ESX и включите VM.
- 3 Войдите на консоли ESX как root.
- 4 Переименуйте файлы VMDK:
`mv <current VMDK path> <renamed VMDK path>`
- 5 Подключитесь к системной консоли FAS (через SSH, Telnet, или консольный кабель).
- 6 Восстановите файл VMDK из Snapshot-копии:
`snap restore -t file -s <snapshot-name> <original VMDK path>
<original VMDK path>`
- 7 Откройте VirtualCenter.
- 8 Выберите ESX и запустите виртуальную машину.
- 9 Убедитесь, что вы восстановили правильную версию. Залогиньтесь в VM и проверьте, что система восстановлена в нужном вам состоянии, на нужный момент времени.
- 10 Войдите на консоли ESX как root.
- 11 Удалите переименованные файлы VMDK:
`rm <renamed VMDK path>`

12.5 ВОССТАНОВЛЕНИЕ ВИРТУАЛЬНОЙ МАШИНЫ ИЗ SNAPSHOT-КОПИИ RDM

RDM предлагает наибо́льший метод восстановления VM из Snapshot-копии. Вкратце этот процесс состоит из выключения VM, восстановления RDM LUN, и включения VM. Выполните следующие шаги.

- 1 Откройте VirtualCenter.
- 2 Выберите хост ESX и выключите VM.
- 3 Подключитесь к системной консоли FAS (через SSH, Telnet, или кабель консоли).
- 4 Склонировать исходный LUN из ближайшей Snapshot-копии:
`lun clone create <original LUN path> -b <original LUN path>
<Snapshot name>`
- 5 Переведите исходную версию LUN в offline:
`lun offline <LUN path>`

- 6 Привяжите клонированный LUN и включите его в online:
`lun online <LUN path>`
`lun map <LUN path> <igroup> <ID>`
- 7 Откройте VirtualCenter.
- 8 Выберите хост ESX и включите VM.
- 9 Проверьте, что восстановлена правильная версия. Войдите в VM и проверьте, что система восстановлена на нужный момент времени.
- 10 Подключитесь к системной консоли FAS (через SSH, Telnet, или кабель консоли).
- 11 Удалите исходный LUN и отделите клон в самостоятельный LUN:
`lun destroy -f <original LUN path>`
`lun clone split start <cloned LUN path>`
- 12 Переименуйте клонированный LUN именем исходного LUN (если необходимо):
`lun mv <cloned LUN path> <original LUN path>`

13. ПРИЛОЖЕНИЕ 2: ПРИМЕР HOT BACKUP SNAPSHOT SCRIPT

Этот скрипт позволяет вам легко провести резервное копирование виртуальных машин на уровне datastore. Это значит, что виртуальные машины должны быть сгруппированы в датасторы на основании политик снэпшотов и SnapMirror backup, позволяя создавать множественные точки восстановления с минимальными усилиями. Бизнес-критичный сервер приложений в виртуальной машине может автоматически создавать снэпшот-копии с любой желаемой частотой, отличной от базового расписания для тестировочной или любой другой некритичной системы. Скрипт также позволяет создавать множественные версии снэпшотов.

Этот скрипт создает управляемый, консистентный бэкап виртуальных машин в системе VMware Virtual Infrastructure 3 используя технологию NetApp Snapshot. Он приводится в качестве примера, и легко может быть изменен, для соответствия нуждам вашей системы.

Для примера продвинутого скрипта, использующего этот базис, смотрите VIBE, размещенный на NetApp ToolChest.

Резервное копирование виртуальных машин с помощью этого скрипта осуществляет следующее:

- Замораживание (Quiesce) всех VMов на заданном datastore
- Создание NetApp Snapshot-копии
- Наложение Redo-логов и возвращение файлов виртуальных дисков в состояние read-write

```
#!/bin/sh
#
# Example code which takes a snapshot of all VMs using the VMware
# vmware-cmd facility. It will maintain and cycle the last 3 Snapshot copies.
#
# This sample code is provided AS IS, with no support or warranties of any
# kind, including but not limited to warranties of merchantability or
# fitness of any kind, expressed or implied.
#
# 2007 Vaughn Stewart, NetApp
#
# -----
PATH=$PATH:/bin:/usr/bin
# Step 1 Enumerate all VMs on an individual ESX Server, and put each VM in hot
# backup mode.
for i in `vmware-cmd -l`
do
vmware-cmd $i createsnapshot backup NetApp true false
done
# Step 2 Rotate NetApp Snapshot copies and delete oldest, create new,
# maintaining 3.
```



```
ssh <Filer> snap delete <esx_data_vol> vmsnap.3
ssh <Filer> snap rename <esx_data_vol> vmsnap.2 vmsnap.3
ssh <Filer> snap rename <esx_data_vol> vmsnap.1 vmsnap.2
ssh <Filer> snap create <esx_data_vol> vmsnap.1
# Step 3 Bring all VMs out of hot backup mode,
for i in `vmware-cmd -l`
do
vmware-cmd $i removesnapshots
done
```

14. ССЫЛКИ

Total Cost Comparison: IT Decision-Maker Perspectives on EMC and NetApp Storage Solutions in Enterprise Database Environments

Wikipedia RAID Definitions and Explanations

VMware Introduction to Virtual Infrastructure

VMware ESX Server 3i Configuration Guide

VMware Storage/SAN Compatibility Guide for ESX Server 3.5 and ESX Server 3i.

VMware VMworld Conference Sessions Overview

VMware Recommendations for Aligning VMFS Partitions

VMware Basic System Administration Guide

NetApp VMInsight with SANscreen

NetApp TR3612: NetApp and VMware Virtual Desktop Infrastructure

NetApp TR3515: NetApp and VMware ESX Server 3.0: Building a Virtual Infrastructure from Server to Storage

NetApp TR3482: NetApp and VMware ESX Server 2.5.x

NetApp TR3001: A Storage NetApp

NetApp TR3466: Open Systems SnapVault (OSSV) Best Practices Guide

NetApp TR3347: FlexClone Volumes: A Thorough Introduction

NetApp TR3348: Block Management with Data ONTAP 7G: FlexVol, FlexClone, and Space Guarantees

NetApp TR3446: SnapMirror Best Practices Guide

RAID-DP: NetApp Implementation of RAID Double Parity

15. ИСТОРИЯ ИЗМЕНЕНИЙ

Version 1.0	May 2006	Original document
Version 2.0	January 2007	Major revisions supporting VI3
Version 2.1	May 2007	Updated VM Snapshot script and instructions
Version 3.0	September 2007	Major revision update
Version 3.1	October 2007	Minor corrections, added NFS snapshot configuration requirement
Version 4.0	March 2008	Major revision update
Version 4.1	July 2008	Minor updates
Version 4.1.1	August 2008	Minor updates
Version 4.2	September 2008	Added VMware co-branding and patch ESX350-200808402-BG
Version 4.3	November 2008	Added VMware KB 2239 update and patch ESX350-200808401-BG
Version 4.4	December 2008	Added support for ESX 3.5 update 3

© 2008 NetApp. All rights reserved. Specifications are subject to change without notice. NetApp, the NetApp logo, Go further, faster, Data ONTAP, FilerView, FlexClone, FlexVol, MultiStore, RAID-DP, SnapMirror for Open Systems, SANscreen, SnapDrive, SnapMirror, SnapRestore, Snapshot, SnapVault, and WAFL are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Linux is a registered trademark of Linus Torvalds. Microsoft and Windows are registered trademarks of Microsoft Corporation. VMware and VMotion are trademarks or registered trademarks of VMware, Inc. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.