

Использование систем ESVA iSCSI в среде VMware vSphere 4

Пример применения

Краткое содержание

В этой статье описывается процесс настройки систем хранения данных Infortrend ESVA iSCSI в среде VMware vSphere4 для достижения высокой эффективности, гибкости и готовности данных в виртуализованных дата центрах.

Виртуализация VMware

Понятие виртуализации возникло в 60-х годах, однако не было востребовано в архитектуре x86 вплоть до 90-х годов. Начиная с 80-х годов, серверы x86 стали широко применяться в IT инфраструктуре, так как они значительно дешевле компьютеров типа mainframe. Эти распределенные вычислительные системы снижают эксплуатационные расходы, однако становятся источником других проблем: плохого использования инфраструктуры, увеличения стоимости ее физических элементов и расходов на администрирование, недостаточной защиты от отказов и аварий и т.д. Виртуализация стала эффективным средством борьбы с этими проблемами.

Основой технологии VMware является ESX Server.

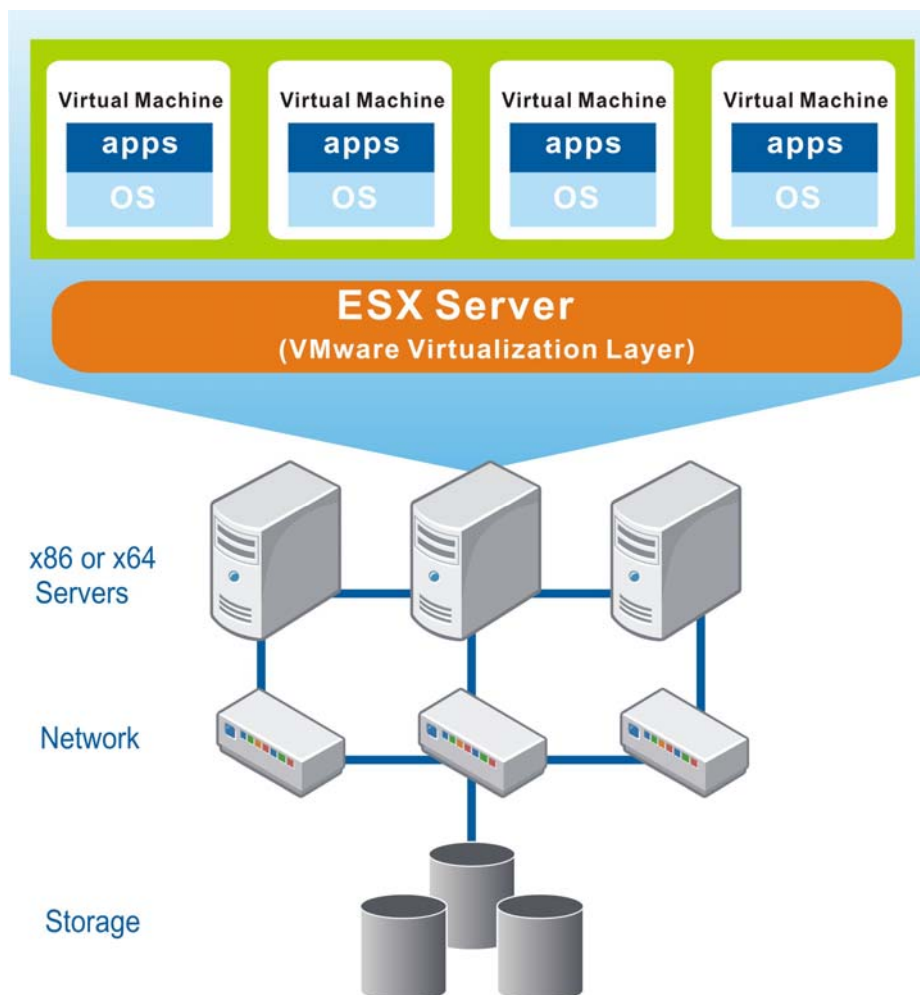


Рис. 1. VMware ESX Server

Будучи установленным на базовый сервер x86 или x64, VMware ESX Server создает слой виртуализации в ОС хоста для того, чтобы объединить все аппаратные ресурсы, в том числе процессоры, память, хранилище и сеть, и затем предоставить эти ресурсы виртуальным



машинам (виртуальным серверам), работающим на физическом сервере. Каждая виртуальная машина может иметь свою ОС и работать со своими приложениями. За счет разделения ресурсов между многими виртуальными машинами пользователь может существенно улучшить их использование и, следовательно, значительно снизить затраты на создание и эксплуатацию физической инфраструктуры дата центров.

Кроме оптимизации использования ресурсов, виртуализация VMware также упрощает развертывание и администрирование системы. Так как развертывание виртуальных машин не связано непосредственно с физическими объектами, то оно может быть выполнено в течение нескольких часов или даже минут. После развертывания менеджер может легко следить за состоянием всего виртуального дата центра через одну общую панель управления. В случае выхода из строя любого из физических устройств возможности VMware могут обеспечить непрерывное функционирование системы.

Системы хранения Infortrend ESVA (Enterprise Scalable Virtualized Architecture) в виртуализованной среде VMware

Семейство Infortrend ESVA является передовым решением для FC и iSCSI SAN предприятий среднего бизнеса. Эти системы с инновационной конструкцией и всеобъемлющими средствами обработки данных, отличающиеся также приемлемой стоимостью, полностью отвечают требованиям по производительности, надежности и возможностям наращивания, предъявляемым к хранилищам для особо важных применений. В системах с архитектурой ESVA (Enterprise Scalable Virtualized Architecture) все основные функции, в том числе виртуализация хранилища, тонкая настройка, распределенный баланс нагрузок, автоматическая миграция данных, приоритетный доступ к томам, создание снимков данных и репликация объединены в одно целое. Дополнив виртуальную инфраструктуру VMware виртуализованным хранилищем ESVA, пользователь может в полной мере ощутить преимущества оптимального возврата инвестиций, упрощения инфраструктуры хранилищ и достижения максимальной производительности.

Оптимальный возврат инвестиций

С помощью технологии виртуализации емкость и вычислительная мощность нескольких систем ESVA могут быть объединены в общий пул хранилищ. Для более эффективного использования объединенной емкости пула хранилищ массивы ESVA поддерживают тонкую настройку изначально присущей им виртуальной архитектуры. Необходимая емкость динамически назначается для работающих приложений как раз в тот момент, когда ее нужно использовать для записи данных. Это намного уменьшает эксплуатационные расходы, во-первых, за счет минимизации пространства,

мощности и затрат на охлаждение больших и обычно недоиспользуемых томов данных в традиционной среде хранения и, во-вторых, за счет отодвигания на более поздние сроки покупок дополнительного оборудования. Кроме рационального использования емкости системы семейства ESVA обеспечивают также эффективное использование полосы пропускания. Зная, что не все приложения равноценны, Infortrend снабжает ESVA интеллектуальным механизмом арбитража доступа. В результате все приложения, подключенные к одному пулу хранилищ, гарантированно получают идеально подходящий для них уровень обслуживания.

Упрощение инфраструктуры хранилищ

Пул хранилищ, который состоит из систем ESVA, значительно упрощает управление, так как он имеет только одну точку администрирования. Нарращивание ESVA пула хранилищ также является очень простой задачей. Чтобы увеличить емкость, вы можете нарастить подсистемы ESVA, входящие в пул, путем подключения к ним корпусов расширения. Если вы хотите увеличить емкость и поднять производительность «одним выстрелом», вы можете также выбрать вариант расширить виртуализированную платформу, добавляя к ней ESVA массивы. Все процедуры наращивания и настройки могут выполняться в режиме online. Когда добавляется новая подсистема, срабатывает механизм баланса нагрузок, который динамически распределяет потоки данных между подсистемами пула хранилищ, так что обрабатываемая мощность растет линейно. Мощность системы, возрастающая в несколько раз вместе с наращиванием емкости, удовлетворит любые запросы даже самых требовательных приложений. Если вы удаляете ESVA массив из пула, то с помощью того же механизма баланса нагрузок потоки данных автоматически перераспределяются так, чтобы сохранить оптимальную производительность без перерыва в обслуживании.

Достижение максимальной производительности

В условиях современного бизнеса даже кратковременная остановка системы означает не только потери прибыли, но может сильно повредить репутации компании, вплоть до прекращения бизнеса как такового. Революционная архитектура ESVA исключает плановые остановки для наращивания хранилища. Чтобы обеспечить непрерывность бизнеса, ESVA имеет возможности репликации. Экономно расходующие дисковое пространство снимки могут служить дискретными точками возврата, отталкиваясь от которых, могут быть восстановлены файлы и предыдущие данные. Что касается полных копий, созданных внутри пула или на подсистемах из других пулов хранилищ, то они тоже легко могут быть использованы приложениями, работающими на хосте, чтобы возобновить обработку информации, когда оригинальные данные повреждены или утрачены. Заранее спланировав и разместив снимки данных и их полные копии, вы можете обеспечить наивысшую защиту ваших данных и минимизировать простои в случае, когда хранилище пострадает от логических ошибок, физических ошибок или катастрофических событий.

Чтобы узнать больше о семействе Infortrend ESVA, посетите страницу нашего сайта <http://www.infostor.ru/esva/ESVA23.html>.

Использование систем ESVA iSCSI в среде VMware vSphere 4

С системами семейства Infortrend ESVA iSCSI пользователь может умножить существующие инвестиции в IP сеть и достигнуть простого объединения ресурсов SAN. Когда объем данных экспоненциально растет с ростом бизнеса, мощная, надежная и гибкая iSCSI SAN даст возможность пользователю успешно и с небольшими затратами противостоять постоянно изменяющимся вызовам IT применений. Семейство ESVA iSCSI представлено двумя моделями: ESVA-E20 и ESVA-E60. E20 допускает применение SATA дисков большой емкости для того, чтобы сохранять и защищать данные с оптимальным соотношением цены и объема данных, в то время как E60 предназначена для применений высшего уровня с большими потоками данных, требующих высокой производительности. Обе модели прошли тестирование на совместимость с VMware vSphere4 и могут быть легко интегрированы в среду VMware: <http://www.vmware.com/resources/compatibility/search.php?action=search&deviceCategory=san&productId=1&advancedORbasic=advanced&maxDisplayRows=50&key=&release%5B%5D=13&datePosted=-1&partnerId%5B%5D=121&arrayType%5B%5D=1&rorre=0>.

Планирование ресурсов

Форматы данных

Чтобы тома данных на массивах ESVA были доступны ESX серверам, они должны иметь формат либо VMFS (Virtual Machine File System), либо RDM (Raw Device Mapping). VMFS - это кластерная файловая система VMware собственной разработки. Это наиболее распространенный метод доступа. Если пользователь хочет, чтобы множественные виртуальные машины, работающие на множественных физических серверах, имели доступ к определенному тому, последний должен иметь формат VMFS. Альтернативный способ предоставить виртуальным машинам доступ к томам данных в хранилище - RDM. Способы доступа виртуальных машин к VMFS и RDM томам различаются. Как показано на Рис. 3, виртуальные машины могут напрямую обращаться к виртуальным дискам в формате VMFS, однако доступ к RDM томам возможен только с помощью файла с таблицей адресов, хранящегося на VMFS томе. Этот файл адресов содержит метаданные, которые переадресуют запросы к физическим устройствам.

¹ Максимальный размер RDM тома равен 2 ТБ.

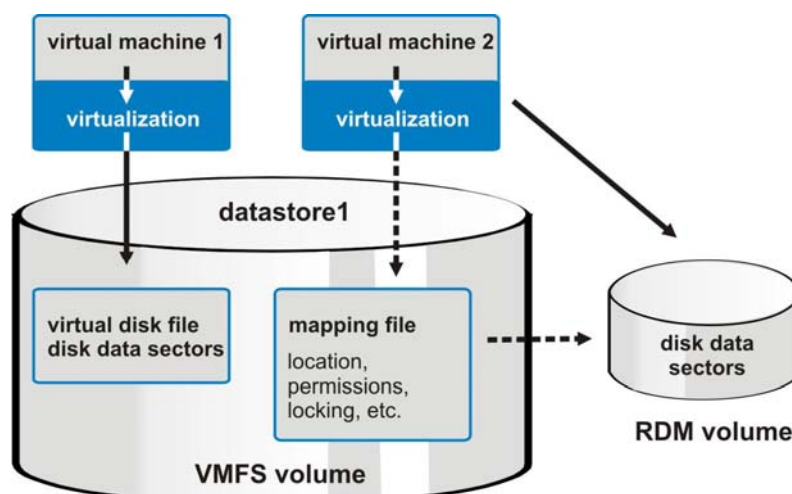


Рис. 2. Различие в доступе к VMFS и RDM томам

Рассматривая RDM том как локальный диск, виртуальная машина может отформатировать его соответствующим образом. RDM особенно полезен в следующих двух случаях:

1. При выполнении виртуальной машиной моментального копирования и копирования тома или других похожих операций в SAN.
2. При использовании Microsoft Clustering Services (MSCS) для создания виртуально-виртуальных или физически-виртуальных кластеров. Агрегированные данные и диски кворума должны быть отформатированы как RDM тома.

Создание VMFS томов

При создании VMFS томов для своих приложений пользователю следует руководствоваться следующими правилами:

1. Загрузочные диски виртуальной машины и данные приложений должны храниться на разных VMFS томах. Большинство I/O запросов к загрузочным дискам подразумевают подкачку файлов и чувствительны ко времени отклика. За счет разделения загрузочных дисков и данных приложений риск увеличения времени отклика из-за одновременного поступления I/O запросов от приложений будет сведен к минимуму.
2. Платформы, обычно применяемые для управления данными предприятий, такие, как Microsoft SQL Server или Oracle, часто используют активные журналы и/или различные структуры восстановления данных для того, чтобы отслеживать их изменения. В случае непредвиденных нарушений в работе приложений или операционной системы эти активные журналы или структуры восстановления данных очень важны для обеспечения восстановления системы и целостности данных. Следовательно, все виртуальные машины, поддерживающие эти базы данных, должны иметь независимые VMFS тома для хранения активных журналов и структур восстановления данных. Более того, если файлы или упомянутые структуры копируются зеркально, то

3. Данные приложений, включая файлы баз данных, должны сохраняться в различных файловых системах VMware. Кроме того, эта файловая система не должна содержать каких бы то ни было структур, чувствительных к восстановлению данных приложений и/или баз данных.
4. Рекомендуется не заполнять VMFS тома более, чем на 80%. В противном случае администратору может не хватить пространства для сохранения данных пользователей и снимков данных для виртуальных машин.

Уровни RAID

RAID массивы ESVA позволяют защитить тома данных с различными уровнями RAID, в том числе RAID 1, RAID 3, RAID 10, RAID 5 и RAID 6. Тома данных в одном и том же массиве могут иметь различные уровни RAID защиты. Ниже приводятся общие рекомендации, как задавать уровни RAID для томов данных в виртуализованной среде VMware.

1. Частота обменов данными с загрузочными томами виртуальной машины обычно невелика, поэтому для них можно выбрать уровень защиты RAID 5.
2. RAID 5 подходит также для защиты виртуальных дисков в большинстве применений. Однако, если предполагается интенсивное ведение журналов, как, например, в финансовых приложениях, то, возможно, RAID 10 будет лучшим вариантом.
3. Инфраструктурные сервера, как, например, сервера доменных имен (Domain Name System - DNS), выполняют большинство операций с использованием центрального процессора и оперативной памяти, следовательно, I/O операции выполняются не часто. Если виртуальная машина применяется как инфраструктурный сервер, то будет полезно снабдить ее томом с защитой RAID 5 в качестве хранилища.
4. Тома с журналами баз данных следует конфигурировать как RAID 10. Если же эти тома, равно как и тома с журналами приложений, копируются зеркально, то источники и приемники должны размещаться на разных наборах дисков (в формате VMFS, если это необходимо).
5. К виртуальным машинам, которые генерируют большие потоки с малым размером блока данных и хаотичными I/O последовательностями, как, например, Microsoft Exchange, для достижения лучшей производительности следует подключать тома с защитой RAID 10.
6. Хранилища больших файловых серверов, заполненные преимущественно статическими файлами, необходимо конфигурировать как RAID 5, так как частота обращений к ним, скорее всего, будет невысокой.

Примерная последовательность действий при настройке

Шаг 1: Добавить iSCSI порты VMkernel к vSwitch

Пользуясь интерфейсом vCenter GUI, выбрать "Configuration tab" в верхнем меню и затем щелкнуть "Networking" в панели "Hardware". Щелкнуть "Properties" для vSwitch, который вы собираетесь использовать в iSCSI трафике.

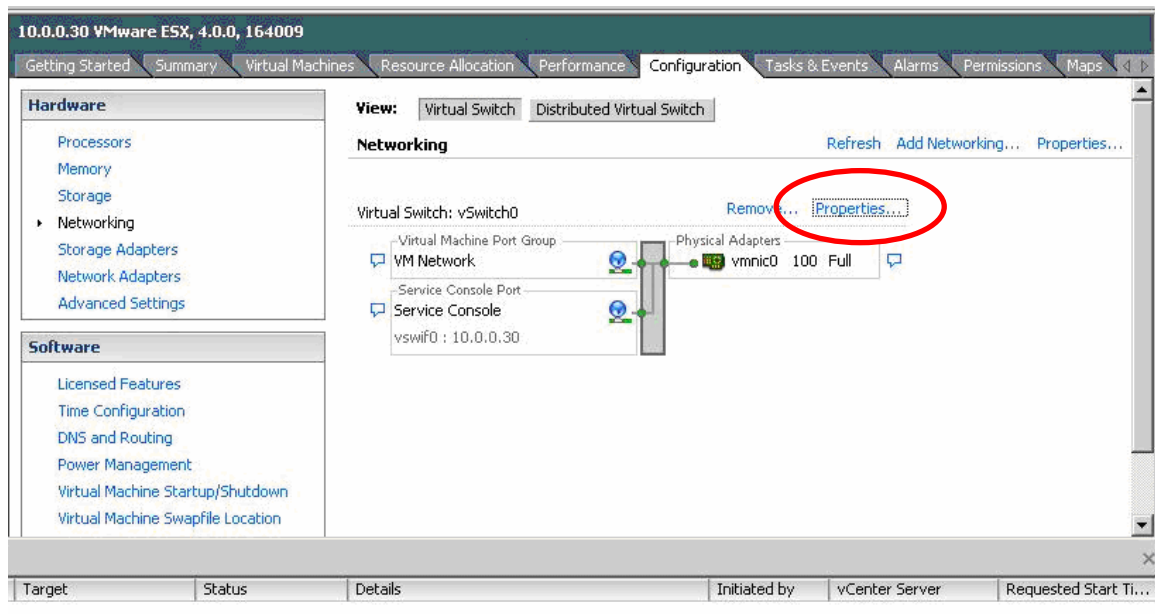


Рис. 3. Доступ к свойствам vSwitch

Щелкнуть "Add" в окне "vSwitch Properties"....

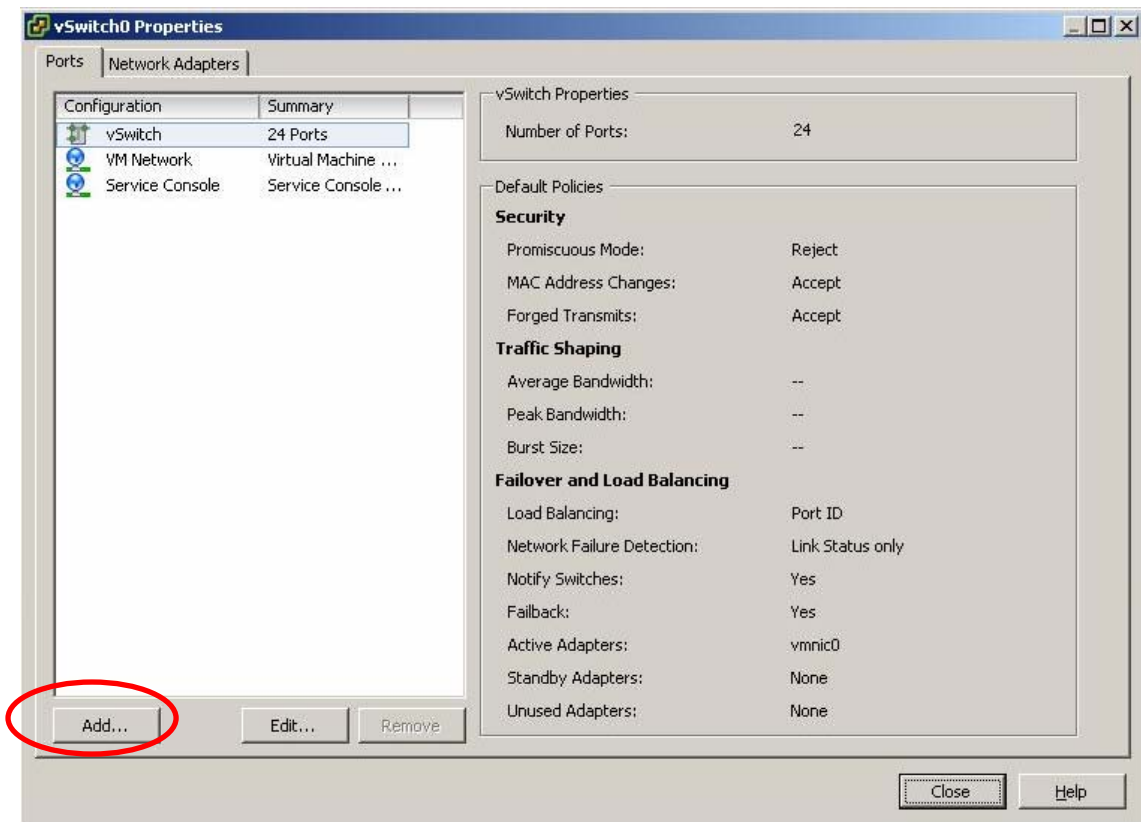


Рис. 4. Свойства vSwitch

Выбрать "VMkernel" как тип соединения в окне "Add Network Wizard".

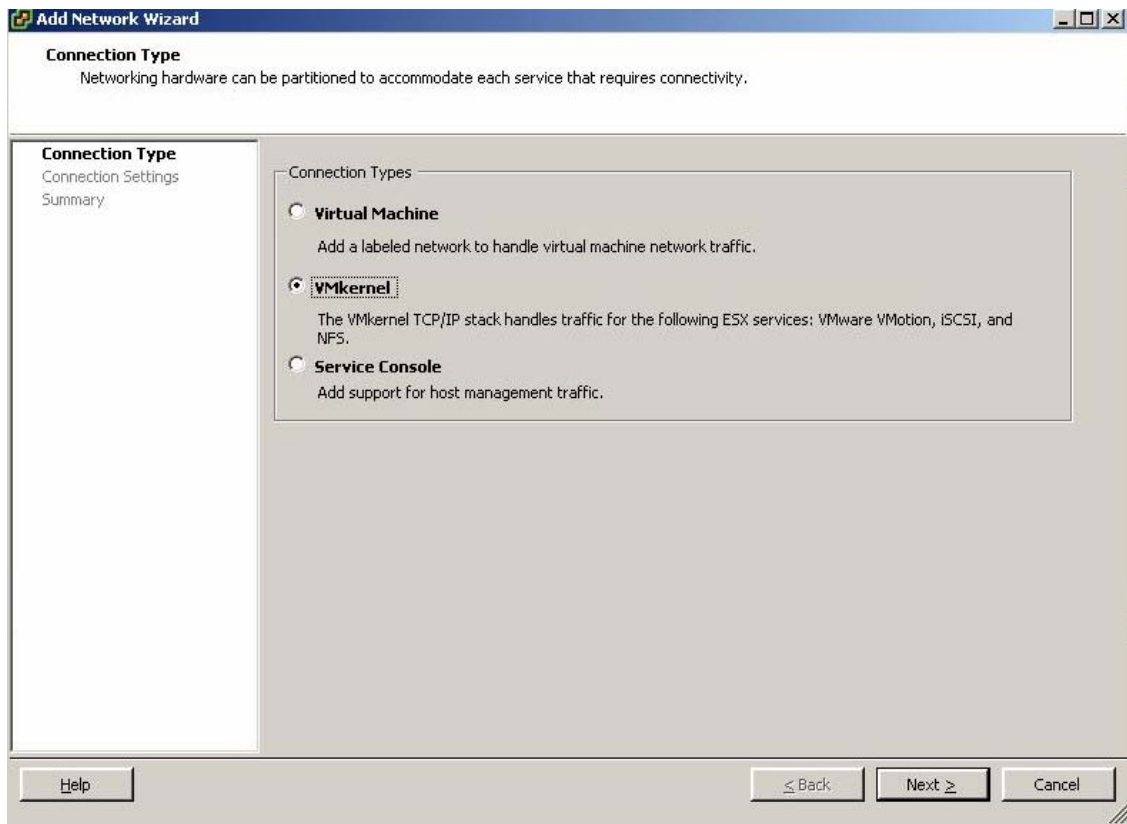


Рис. 5. Выбор VMkernel как типа соединения

После назначения имени сети (Network Label) и настройки IP порт VMkernel будет успешно добавлен к vSwitch. Повторите процедуру, если вы хотите создать другие порты VMkernel.

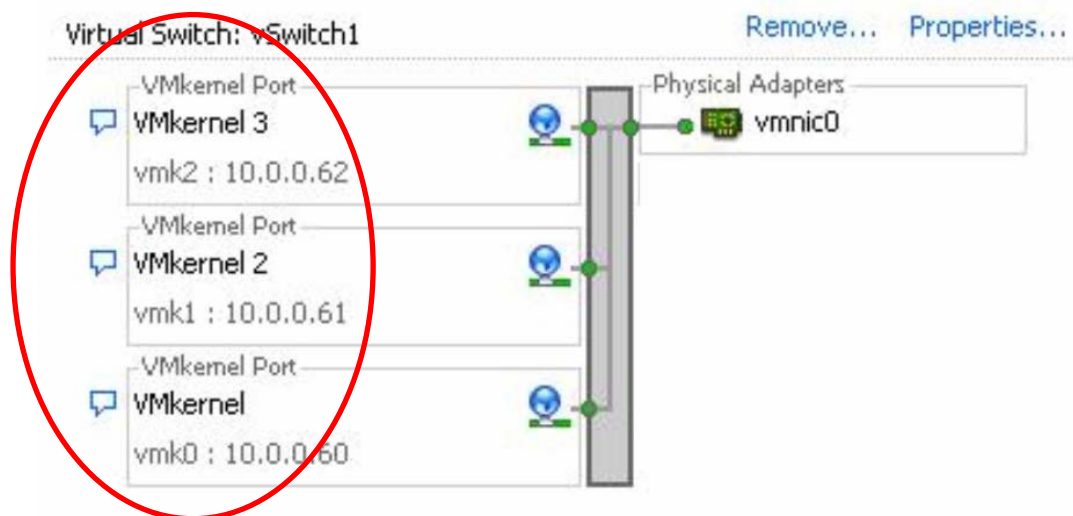


Рис. 6. Порты VMkernel созданы

Примечание: VMware vCenter допускает до восьми подключений к одному тому данных, и каждый сетевой адаптер может быть связан с более чем одним портом VMkernel. Количество портов The number of VMkernel ports you create in this step may vary with your applications needs. For example, if you have two network adapters and would like to associate two VMkernel ports for each of them, you have to create four VMkernel ports in this step.

Шаг 2. Назначение сетевых адаптеров

Щелкнуть "Networking" в окне vCenter GUI в панели "Hardware". Щелкнуть "Properties" для vSwitch, который вы собираетесь использовать для трафика iSCSI. Щелкнуть таблицу "Network Adapters" в окне "vSwitch Properties", затем "Add..." В окне "Add Adapter Wizard" выбрать vmnics, который вы хотите добавить к vSwitch и использовать для iSCSI трафика, затем щелкнуть "Next".

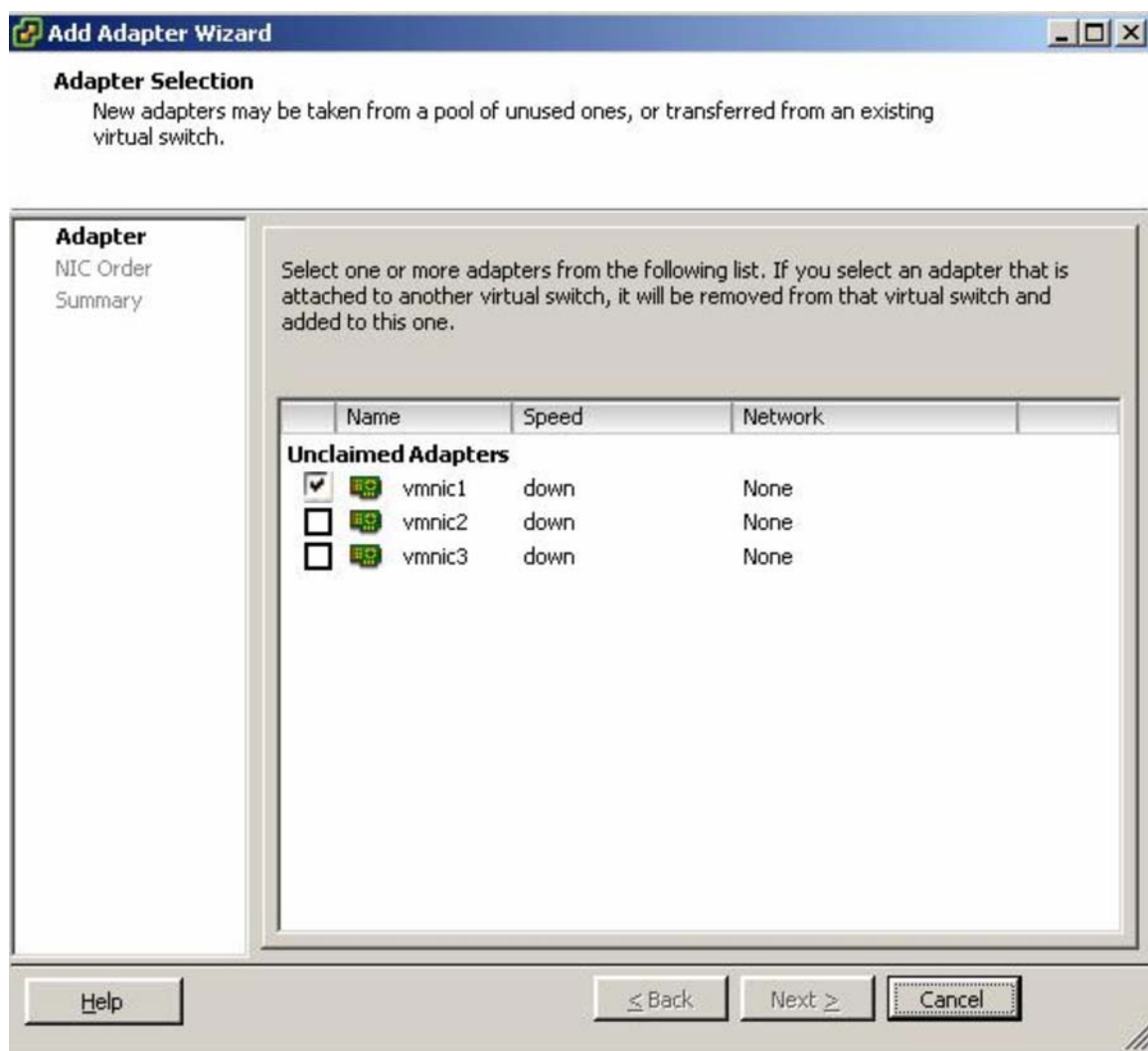


Рис. 7. Выбор адаптера

Настроить порядок обработки отказов, затем щелкнуть "Finish".

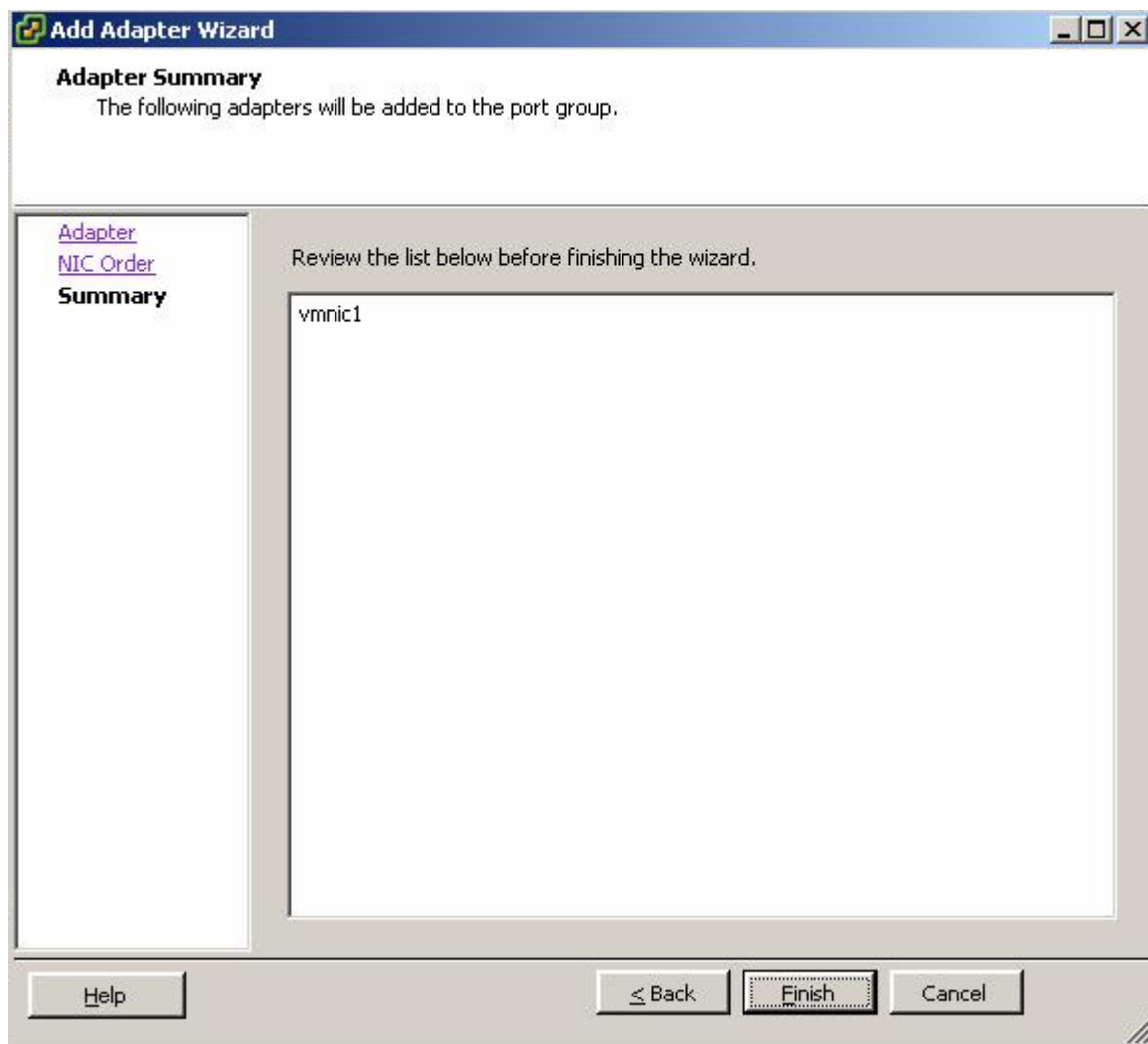


Рис. 8. Завершение добавления адаптера

Теперь адаптер(ы), которые вы выбрали, появятся в окне vCenter GUI в таблице сетевых адаптеров.

Шаг 3. Настройка соответствия портов VMkernel сетевым адаптерам

Щелкнуть "Networking" в окне vCenter GUI в панели "Hardware". Щелкнуть "Properties" для vSwitch. Выбрать нужный из портов VMkernel, затем щелкнуть "Edit...". Щелкнуть таблицу "NIC Teaming" в окне "VMkernel Properties". Выбрать "Override vSwitch Failover Order". По умолчанию все порты VMkernel будут назначены всем NIC, которые вы установили. Чтобы каждый порт VMkernel был сбалансированно подключен только к одному адаптеру, вы должны выбрать адаптер, к которому вы не хотите подключать порт VMkernel, затем щелкнуть кнопку "Move Down", чтобы он появился в списке "Unused Adapters".

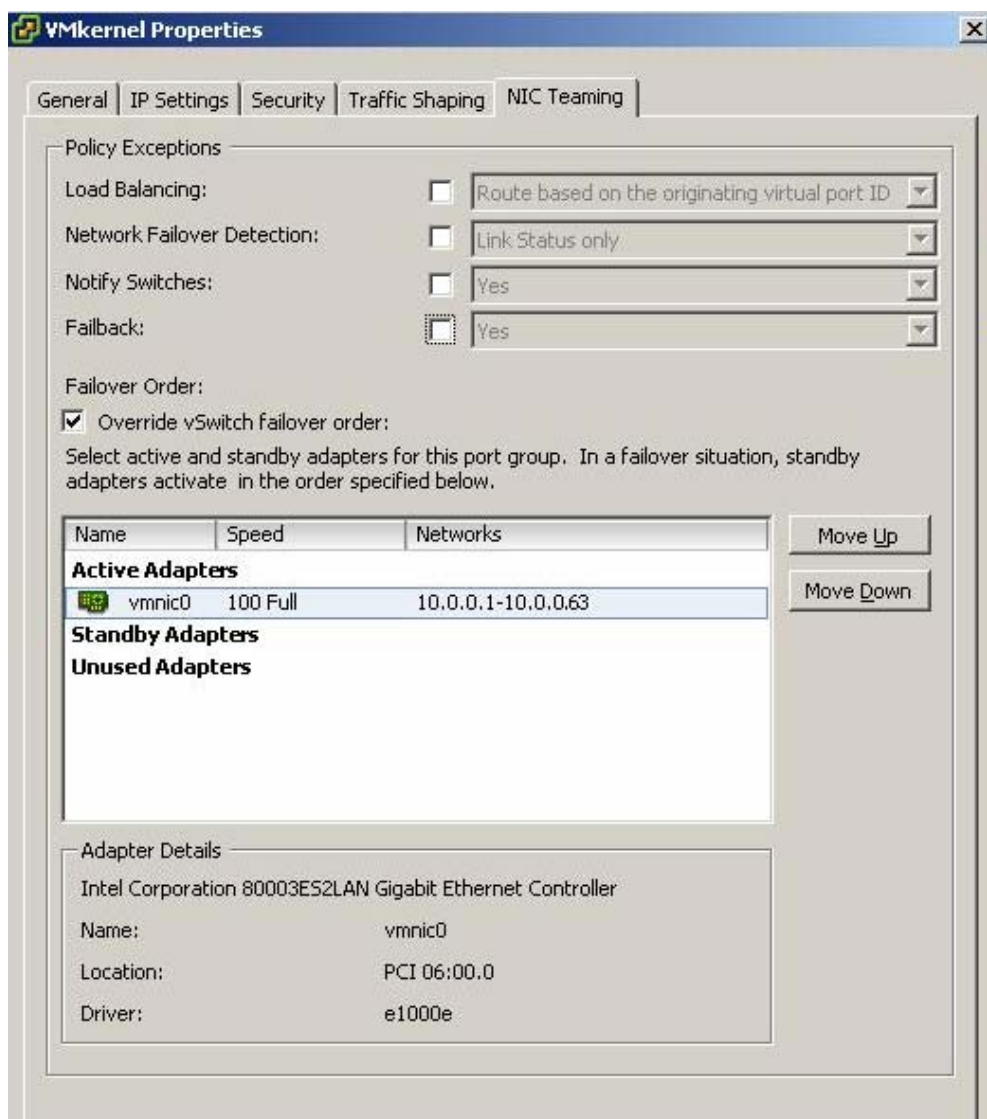


Рис. 9. Свойства VMkernel

Шаг 4. Подключение инициатора VMware iSCSI и настройка идентификации CHAP

Щелкнуть "Storage Adapters" в панели "Hardware" в окне vCenter GUI. Выбрать программный адаптер iSCSI, затем щелкнуть "Properties". Выбрать таблицу "General" в окне "iSCSI Initiator Properties". Щелкнуть кнопку "Configure...", после чего появится окно "General Properties". Выбрать "Enabled" в этом окне, затем щелкнуть "OK".

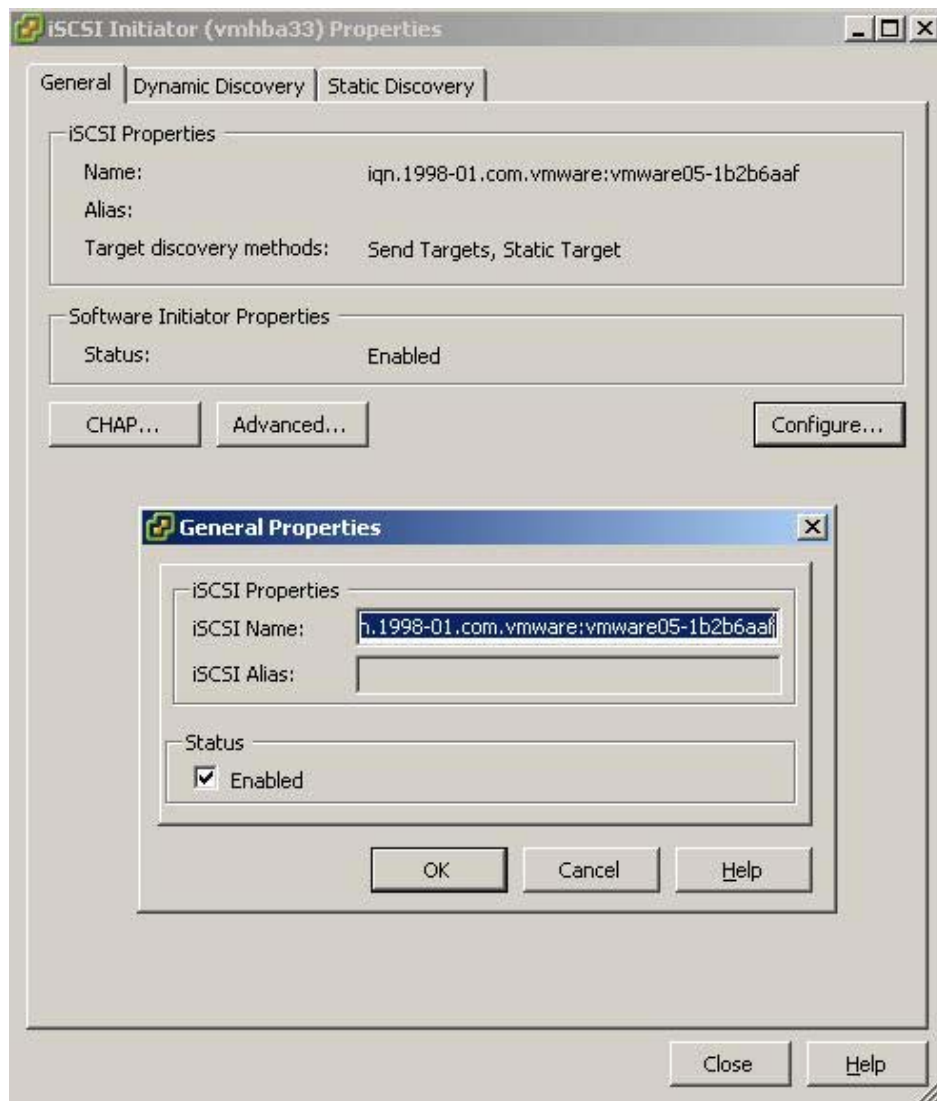


Рис. 10. Подключение инициатора iSCSI

Щелкнуть кнопку "CHAP...", должно появиться окно "CHAP Credentials". VMware ESX4.0 поддерживает как одностороннюю, так и двухстороннюю CHAP идентификацию. Если вы хотите, чтобы только приемники iSCSI идентифицировали хост, выберите "Use CHAP" в выпадающем меню после "Select Option" в разделе установок "CHAP". Если же вы хотите, чтобы хост также идентифицировал приемники iSCSI, выберите select "Use CHAP" в выпадающем меню после "Select Option" в разделе установок "Mutual CHAP", затем введите имя и пароль. После выполнения этих установок соединение может быть успешно установлено только после того, как пройдет CHAP идентификация.

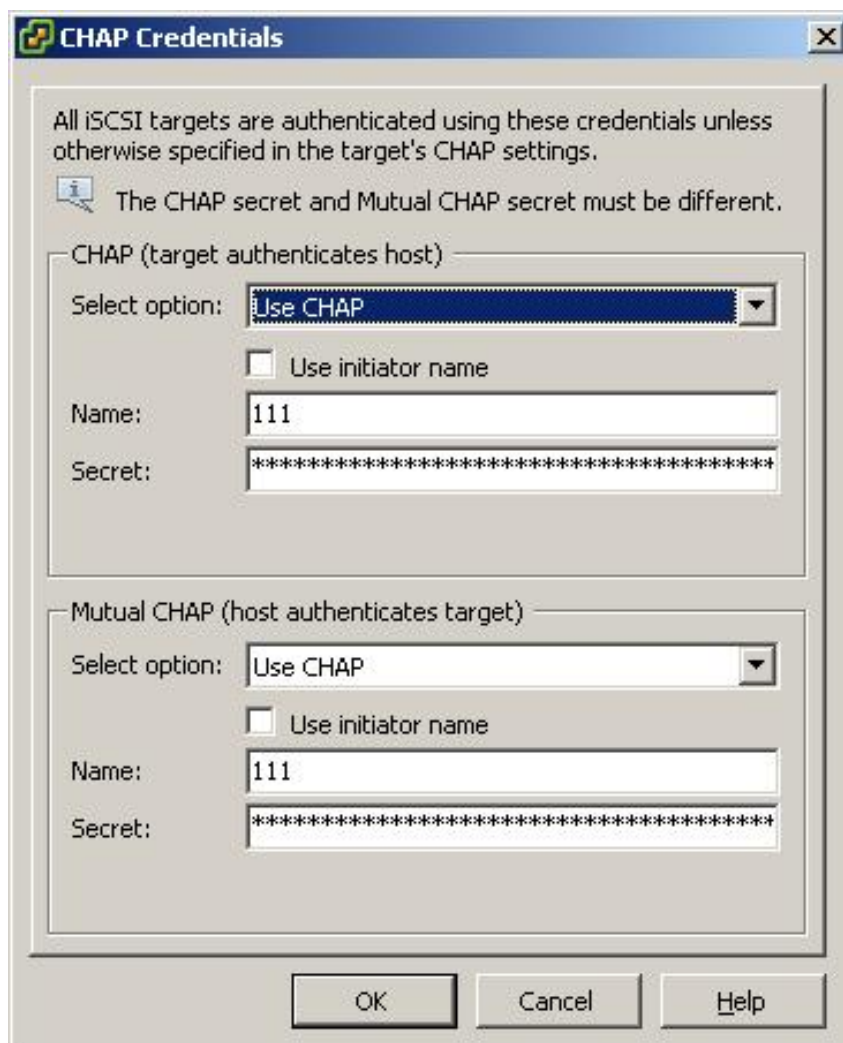


Рис . 11. Разрешение CHAP идентификации

Примечание: Хранилища Infortrend не поддерживают установку различных режимов идентификации для различных приемников. В данном случае режим CHAP идентификации задан на корневом уровне iSCSI инициатора и распространяется на все iSCSI приемники.

Шаг 5. Привязка портов VMkernel к программным инициаторам iSCSI

Этот этап настройки должен выполняться с помощью команд CLI (Command Line Interface). Перед конфигурированием необходимо записать значения vmhba# программного инициатора iSCSI и vmk# каждого порта VMkernel. Первое можно увидеть, щелкнув "Storage Adapters" в панели "Hardware panel" графического интерфейса пользователя (GUI) vCenter.

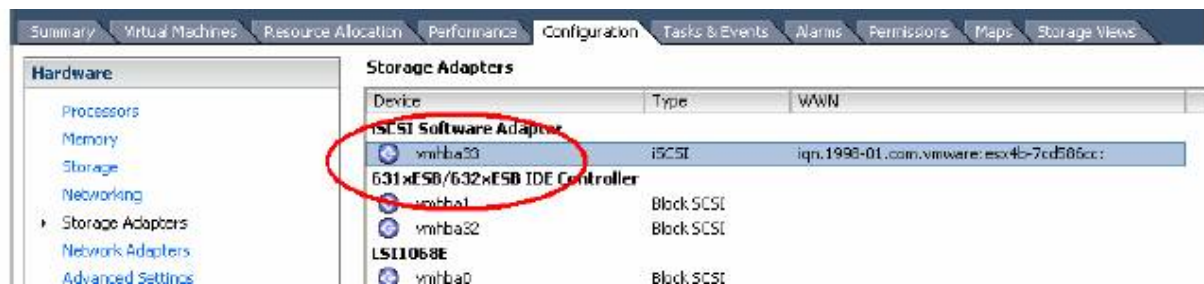


Рис. 12. vmhba# программного адаптера iSCSI

Последнее можно увидеть, щелкнув "Networking" в панели "Hardware". В колонке "vSwitch for iSCSI traffic" вы можете видеть значения vmk# для каждого порта VMkernel.

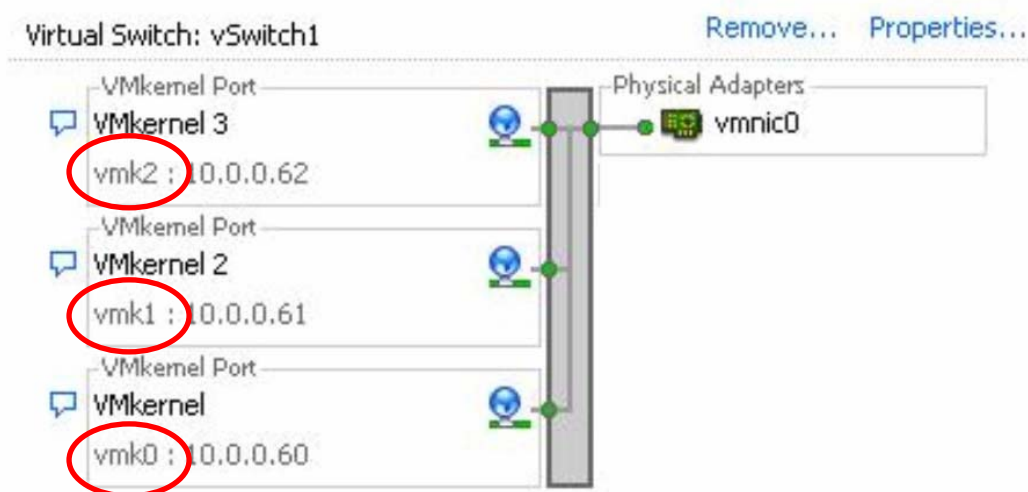


Figure 13. vmk# портов VMkernel

Если вы хотите привязать ghnn vmk0 VMkernel к программному адаптеру iSCSI vmhba33, наберите следующую команду:

```
esxcli swiscsi nic add -n vmk0 -d vmhba33
```

Повторите эту команду до тех пор, пока все порты VMkernel не будут привязаны к адаптеру iSCSI.

Шаг 6. Добавление IP порта канала iSCSI ESVA программному адаптеру iSCSI

Щелкните "Storage Adapters" в панели "Hardware" окна vCenter GUI. Выберите "Select the iSCSI software adapter", затем щелкните "Properties". Выберите "Dynamic Discovery" в окне "iSCSI Initiator Properties". Щелкните "Add...", появится окно "Add Send Target Server". В этом окне ввести IP адреса портов каналов iSCSI вашей системы ESVA.

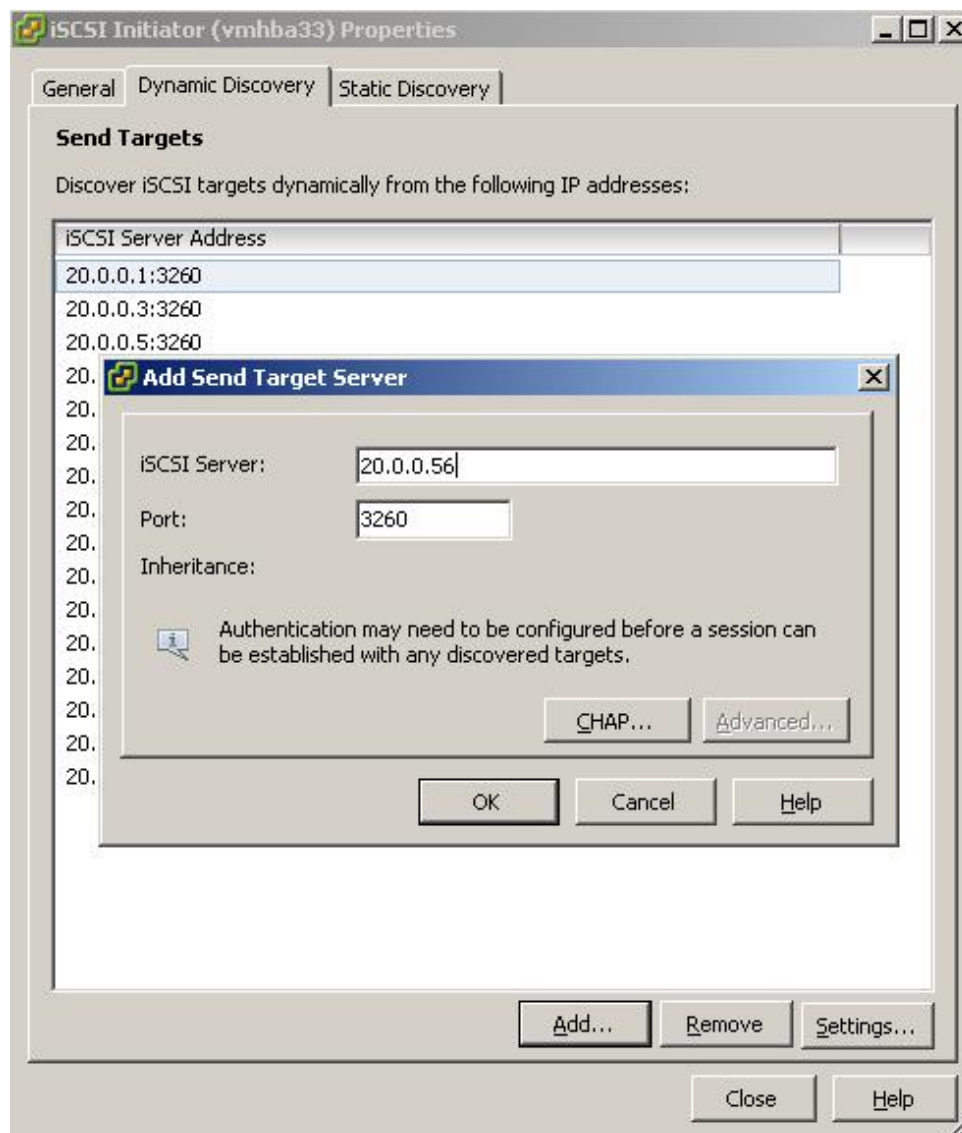


Figure 14. Adding iSCSI Channel Port IP Addresses

Повторять эту процедуру до тех пор, пока не будут добавлены все IP адреса. После этого щелкнуть "Close".

Шаг 7. Создание виртуального тома на ESVA

Этот этап настройки должен выполняться при помощи Менеджера Виртуализации (Virtualization Manager) пакета администрирования SANWatch. Подробности вы найдете в Руководстве Пользователя Менеджера Виртуализации.

Шаг 8. Добавление VMFS Datastore виртуальной машине

Щелкнуть "Storage Adapters" в панели "Hardware" окна vCenter GUI. Выбрать "iSCSI Software Adapter" и щелкнуть "Rescan". В появившемся окне выбрать "Scan for New Storage Devices" и "Scan for New VMFS Volumes", щелкнуть "OK".

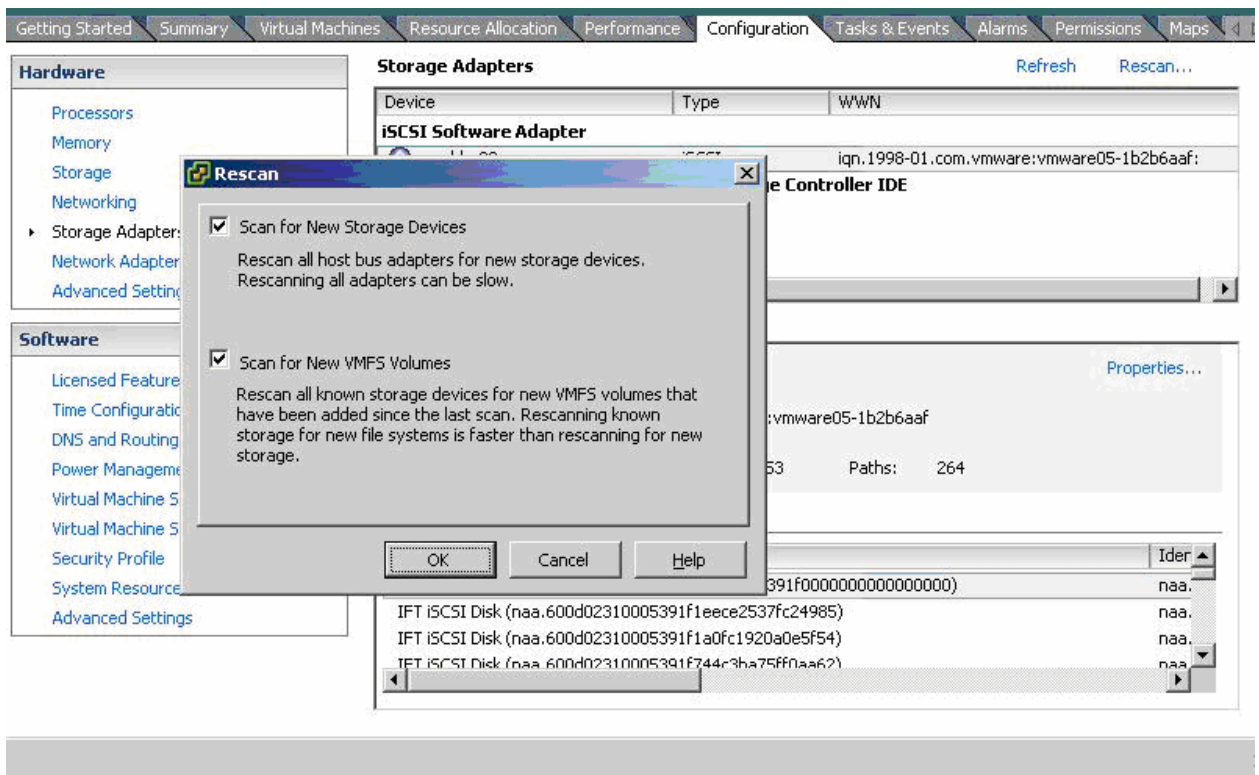


Рис. 15. Сканирование хранилища

Щелкнуть "Storage" в панели "Hardware" окна vCenter GUI. После этого щелкнуть "Add Storage..."

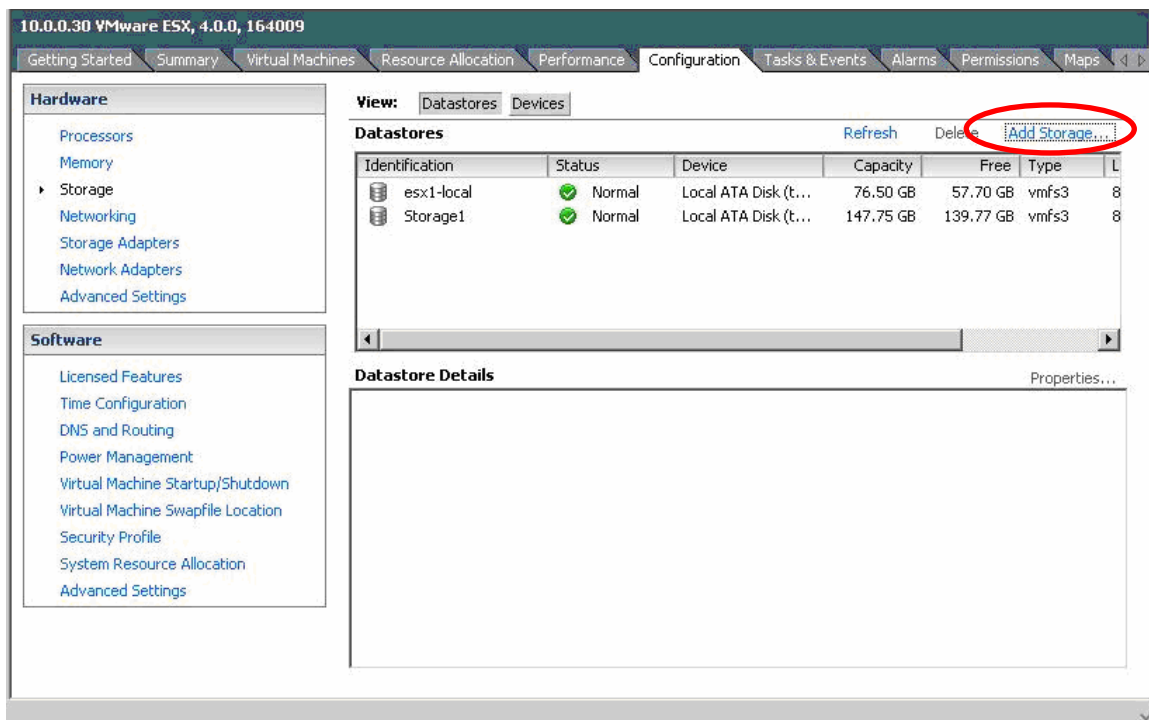


Рис. 16. Добавление хранилища

Должно появиться окно "Add Storage". Сначала следует выбрать "Disk/LUN" в качестве типа хранилища, затем щелкнуть "Next".

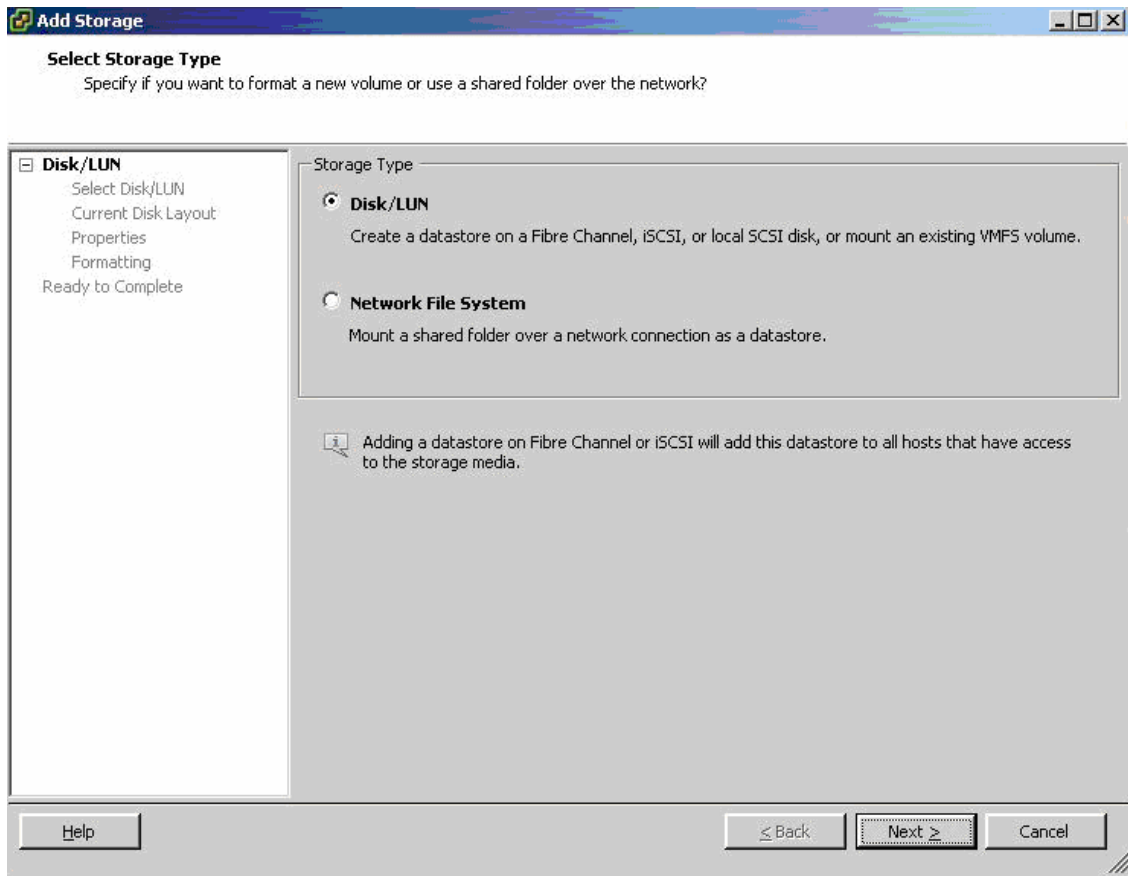


Рис. 17. Выбор Disk/LUN в качестве типа хранилища

Выбрать в списке всех имеющихся iSCSI дисков тот, который вы бы хотели добавить как новое VMFS хранилище данных и щелкнуть "Next".

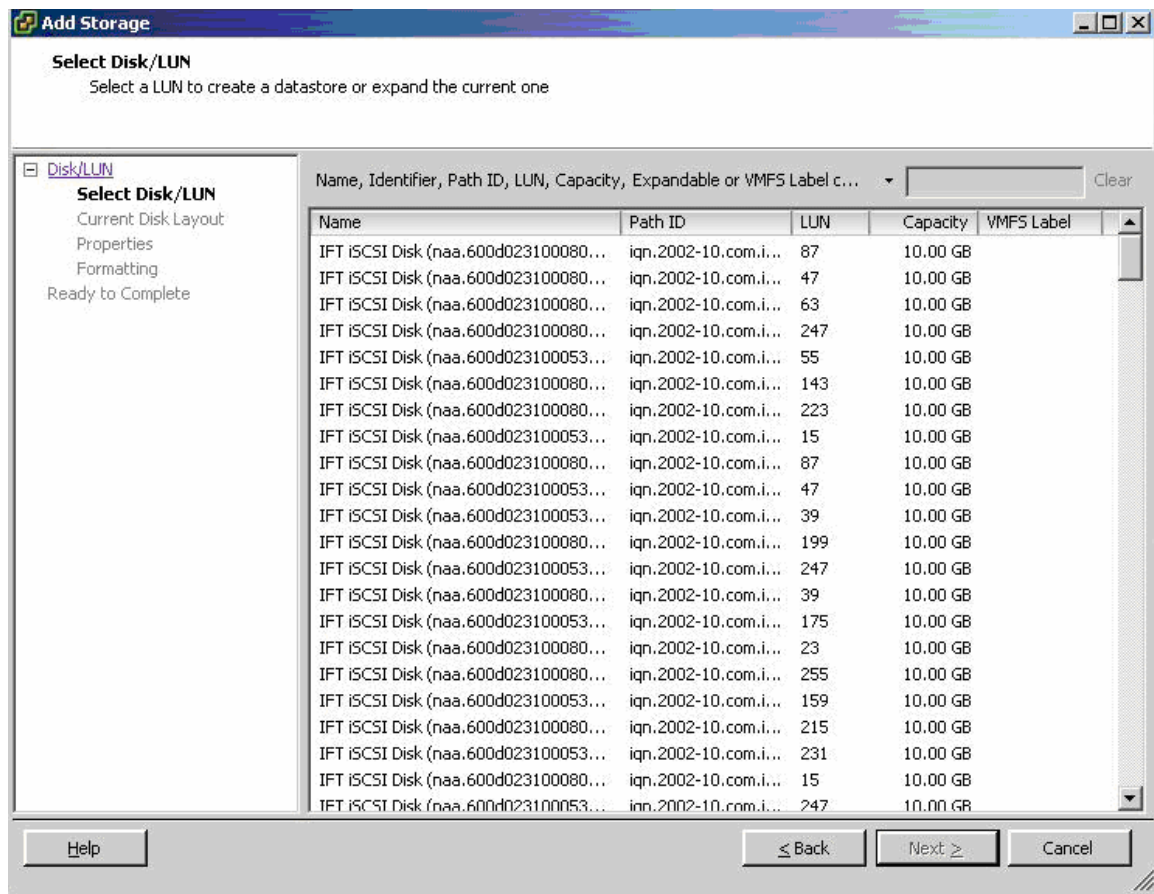


Рис. 18. Выбор iSCSI диска

Процесс конфигурирования завершается введением имени хранилища и максимального размера файла, после этого щелкнуть "Finish".

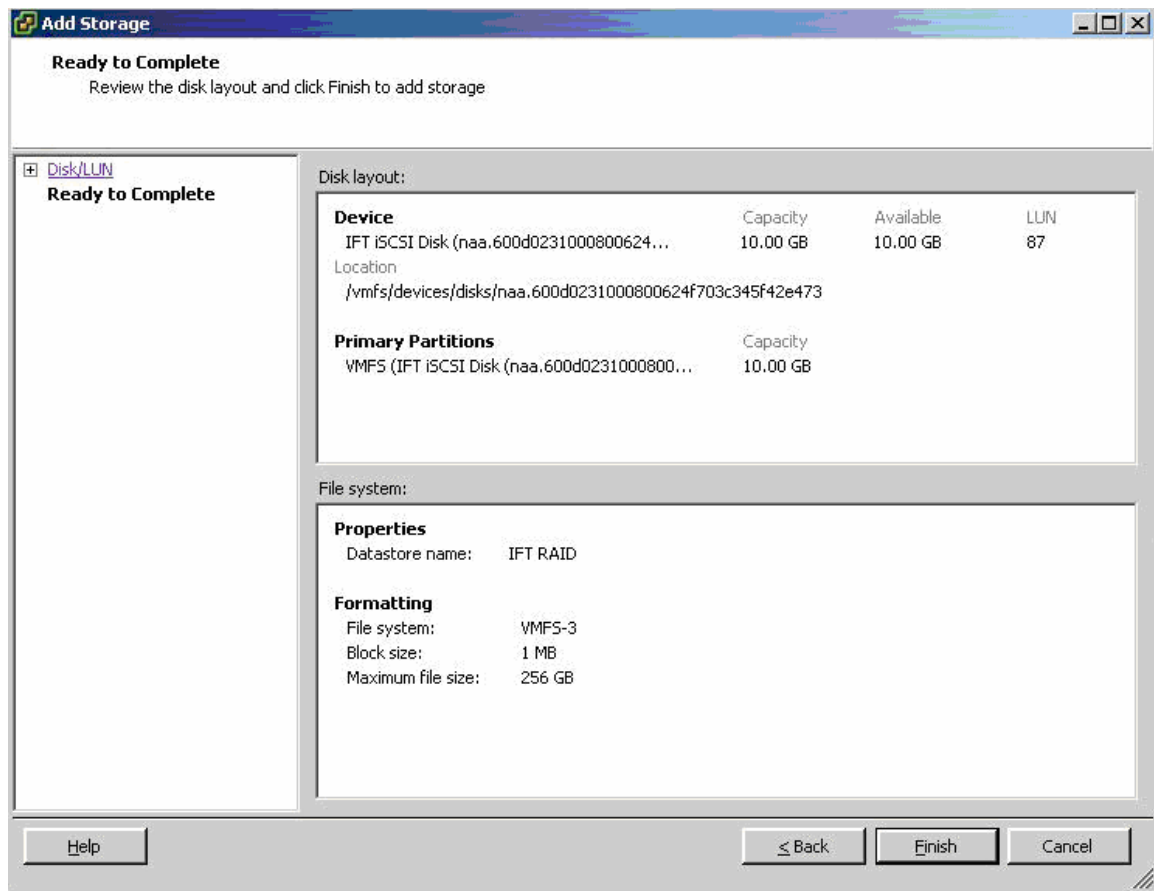


Figure 19. Finishing Datastore Creation Process

Таким образом, новое VMFS хранилище данных создано.

Шаг 9. Подключение встроенного многоканального режима VMware

Щелкнуть "Storage" в панели "Hardware" окна vCenter GUI и выбрать том, для которого вы хотите задать многоканальный режим. Щелкнуть правую кнопку и выбрать "Manage Paths". В появившемся окне отметить правило выбора пути из выпадающего меню, следующего за "Path Selection".

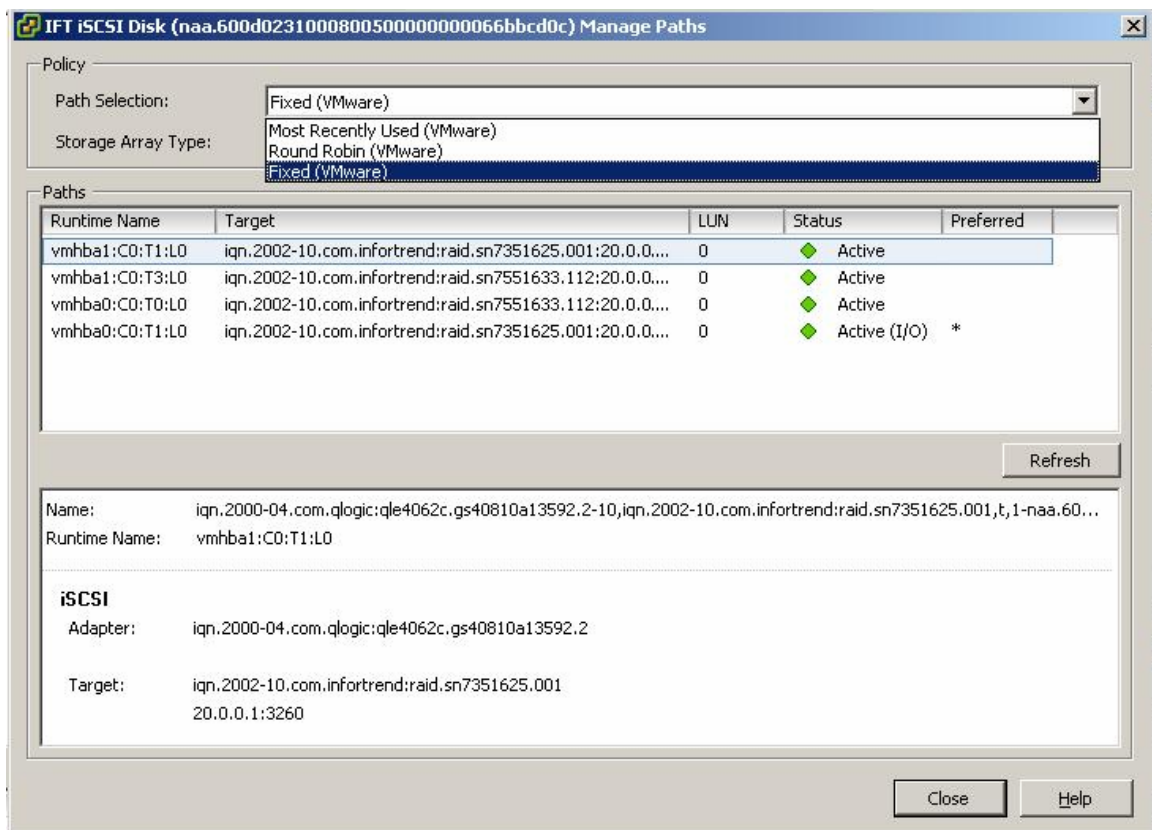


Рис. 20. Правила выбора пути

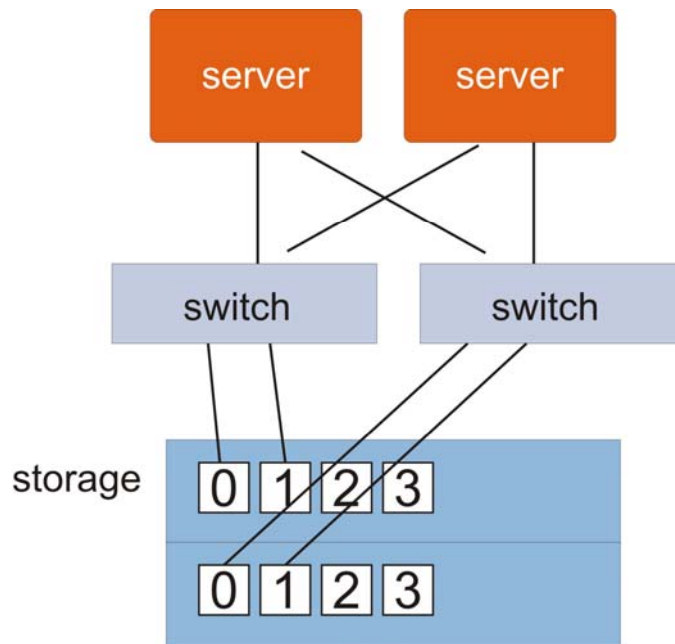
Примечание: Правила выбор могут изменяться в зависимости от требований приложений, однако рекомендуется циклическое чередование, так как оно позволяет равномерно распределить поток данных для этого тома по всем имеющимся путям.

Основные неисправности и часто задаваемые вопросы

1. Какую информацию мне надо предоставить, если мне требуется помощь в устранении неисправности?

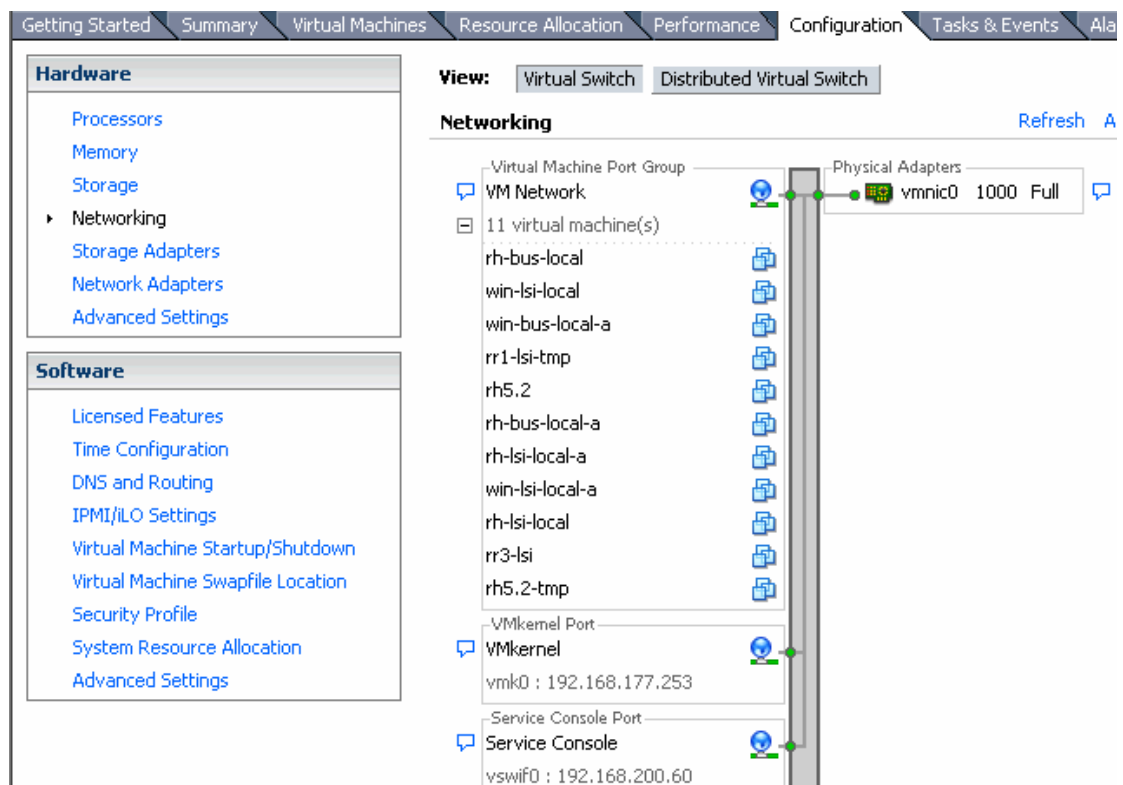
Предоставьте, пожалуйста, следующую информацию:

- Версия ESX сервера (например, ESX4.0, ESX3.5)
- Модель хранилища, версия встроенного ПО и журналы событий
- Топология вашего ESX сервера, переключателей и хранилища, как показано ниже



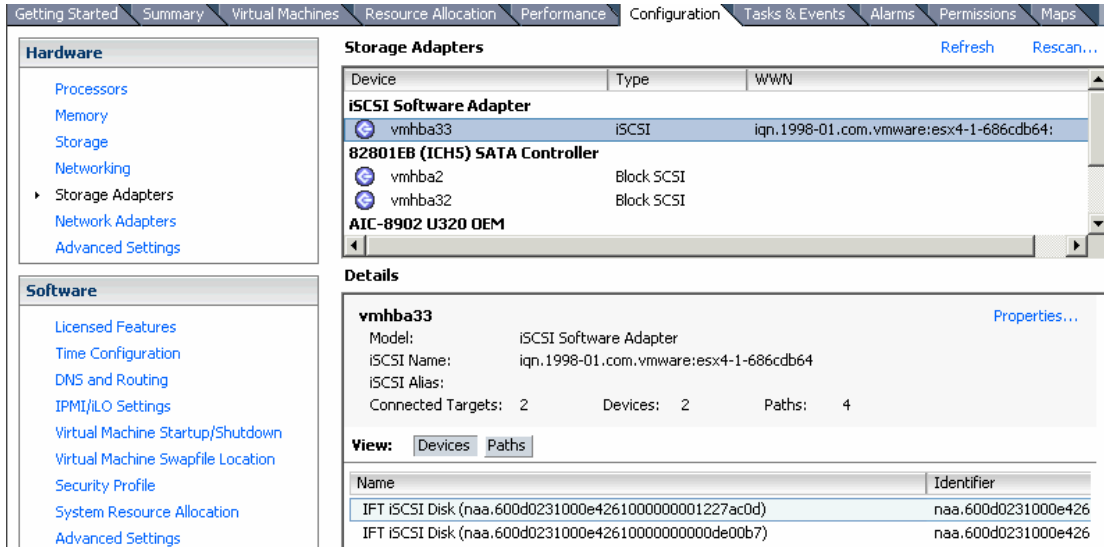
- Конфигурация хранилища, включая partitions LD, виртуальных пулов, виртуальных томов и назначение LUN; все эти данные можно получить через SANWatch
- Описание поведения системы, предшествующего появлению проблемы
- Конфигурация ESX сервера, отраженная в скриншотах "Networking", "Storage Adapters" и "Maps" vCenter/VirtualCenter GUI

Пример: Networking

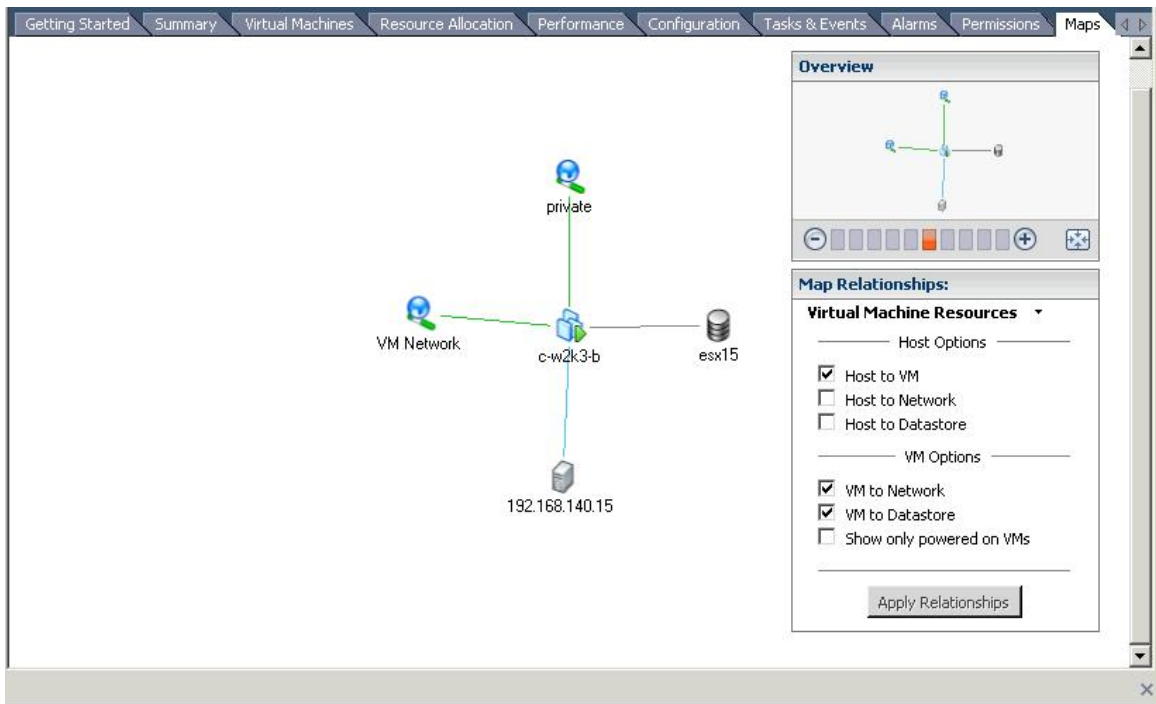




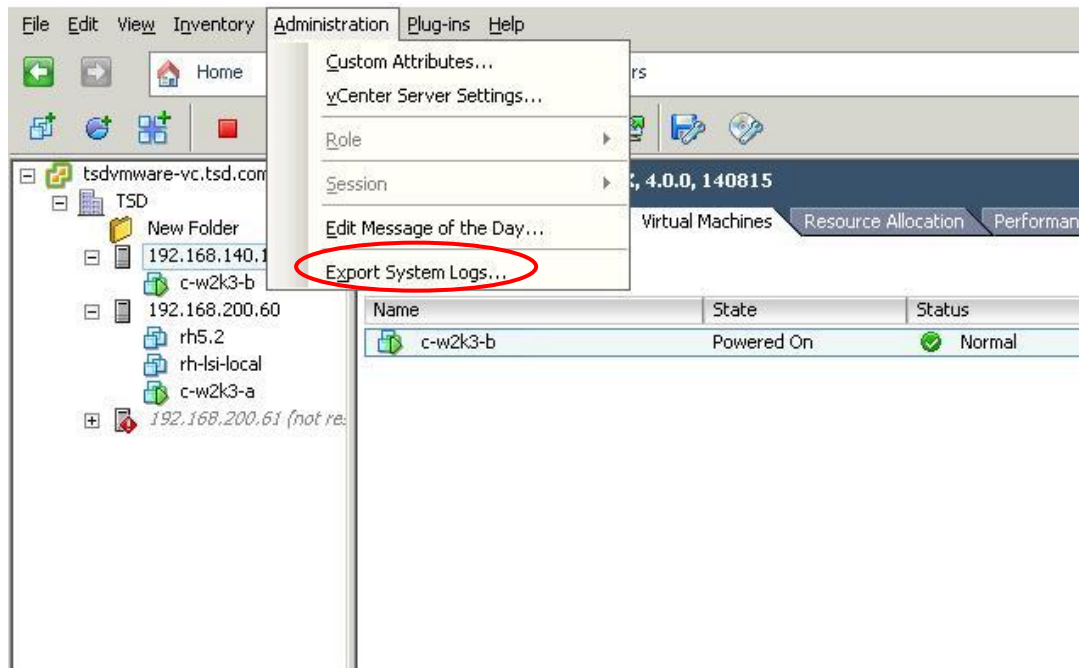
Пример: Storage Adapters



Пример: Maps

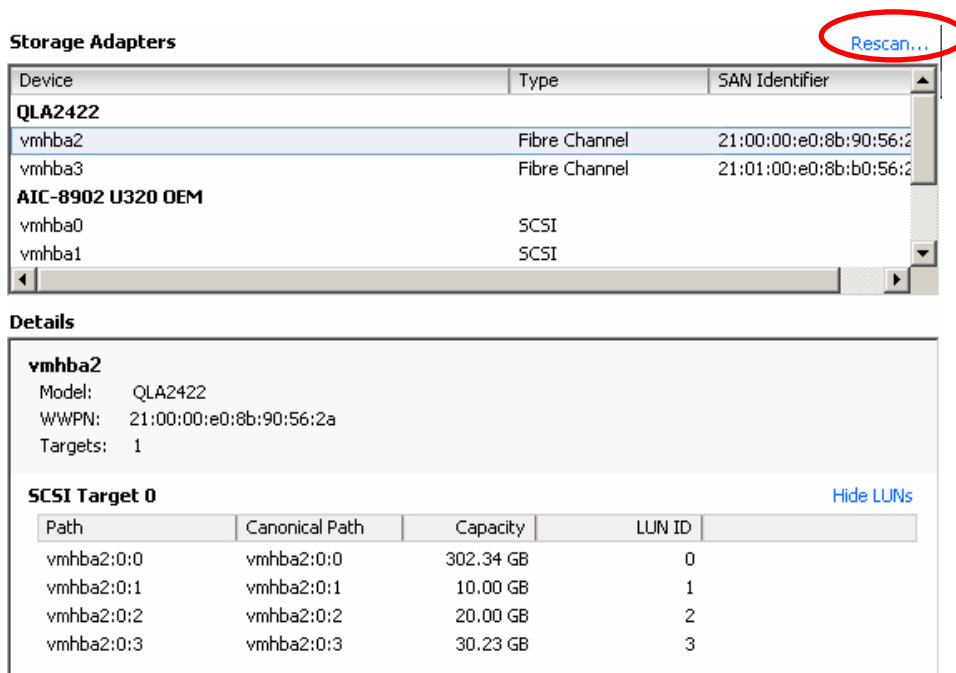


- Журналы событий ESX сервера; вы можете найти их в папке `/var/log/vmkernel` или получить при помощи vCenter/VirtualCenter GUI. Щелкнуть "Administration" в верхнем меню и выбрать "Export System Logs" из выпадающего меню.



2. Почему я не вижу VMFS тома, который я создал ранее?

Пожалуйста, проверьте начала, видите ли вы физическое устройство, использованное для создания VMFS тома в vCenter/Virtual Center GUI. Если нет, проверьте правильность подсоединения кабелей и назначения LUN. Затем выполнить операцию "Rescan" на экране "Storage Adapters".



Если после этого проблема не исчезнет, подготовьте, пожалуйста, данные, перечисленные в вопросе 1, и свяжитесь с нами для дальнейшего рассмотрения.

3. Какие ограничения на конфигурацию существуют в виртуализованной среде VMware? Зайдите, пожалуйста, на http://www.vmware.com/pdf/vsphere4/r40/vsp_40_config_max.pdf, там вы сможете узнать все подробности.
4. Как добиться успешного переключения каналов при отказе одного из избыточных контроллеров? Если вы используете ESX 4.0 с массивами EonStor, имеющими версию встроенного программного обеспечения 3.64, или более позднюю, то система автоматически обработает эту ситуацию без ручного вмешательства. Однако, если вы используете ESX 3.x, следуйте, пожалуйста, процедуре, описанной в примере применения: http://www.infortrend.com/doc/appNoteAPP_VMware_footnote_1117.pdf.
5. Может виртуальная машина мигрировать к другому тому данных без перерыва в работе? Да, виртуальная машина может мигрировать online к другому тому данных. Для более подробного объяснения обратитесь, пожалуйста, к http://www.vmware.com/products/vi/storage_vmotion.html <http://blogs.vmware.com/vi/2008/06/storage-vmotion.html>
6. Если я хочу воспользоваться многоканальным резервированием, должен ли я выполнить какие-то специальные установки на моем хранилище? Должен ли я установить EonPath? Нет, никаких специальных установок не требуется. Вы должны только следовать общей многоканальной конфигурации. Более того, так как VMware имеет встроенные многоканальные функции, нет необходимости устанавливать другие драйверы, включая EonPath, для того, чтобы использовать многоканальное резервирование.

Приложение: Режим Jumbo фреймов

Jumbo фреймы - это одна из новых передовых возможностей, поддерживаемых VMware vSphere ESX4.0. Она позволяет передавать большие пакеты между хостом и SAN, за счет чего значительно возрастает эффективность системы и ее характеристики. В настоящее время пользователи могут разрешить Jumbo фреймы только с помощью команд CLI. Ниже приведена примерная последовательность шагов при настройке.

Примечание: Убедитесь, пожалуйста, что ваше сетевое оборудование поддерживает режим Jumbo фреймов перед тем, как начинать конфигурирование.

Шаг 1. Разрешить передачу Jumbo фреймов через vSwitch

Если вы хотите разрешить Jumbo фреймы для vSwitch1, выполните следующую команду:

```
esxcfg-vswitch -a vSwitch1
```

Чтобы проверить ее выполнение, выполните еще одну команду:

```
esxcfg-vswitch -1
```

После этого вы должны увидеть сообщение, похожее на это:

Switch Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks	vSwitch2
24	1	24	9000			

PortGroup Name	VLAN ID	Used Ports	Uplinks
----------------	---------	------------	---------

Шаг 2. Добавление портов iSCSI VMkernel к vSwitch и разрешение передачи Jumbo фреймов через порты

Чтобы разрешить Jumbo фреймы, вы должны добавить порты iSCSI VMkernel с помощью команд CLI, а не vCenter GUI. Если вы хотите добавить VMkernel порт с именем VMkernel1 к vSwitch1, выполните следующую команду:

```
esxcfg-vswitch -A VMkernel1 vSwitch1
```

Затем задайте IP адрес, Subnet Mask и разрешите Jumbo фреймы для нового порта VMkernel при помощи следующей команды:

```
esxcfg-vmknics -a -i 10.10.0.61 -n 255.255.255.0 -m 9000 VMkernel1
```

Повторите эти шаги для того, чтобы создать другие порты VMkernel. Чтобы проверить успешность этой операции, выполните команду:



esxcfg-vswitch -1

После этого вы должны увидеть сообщение, похожее на это:

Switch Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks vSwitch2
24	4	24	9000		

PortGroup Name	VLAN ID	Used Ports	Uplinks
VMkernel1	0	1	
VMkernel2	0	1	
VMkernel3	0	1	

Теперь режим Jumbo фреймов успешно задан. Остальные шаги настройки для использования ESVA в среде vSphere 4 такие же, как описано выше, в главной части этого руководства.