МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ ИСВЯЗИ

ФАКУЛЬТЕТ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

УДК 004.65:004.45-021.131:378 На правах рукописи

Магистерская диссертация

Преимущества технологии виртуализации в процессе обучения студентов

Магистерская диссертация на соискание

академической степени магистр технических наук по специальности

6М070400 – Вычислительная техника и программное обеспечение

Ковалевский Сергей
Юрьевич

АЛМАТЫ, 2014

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

ФАКУЛЬТЕТ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

Допущен к защите:

зав. кафедрой «Компьютерные технологии»

д. ф.-м. н., профессор _____ Куралбаев З.К.
«___»_____20 __г.

Магистерская диссертация

Преимущества технологии виртуализации в процессе обучения студентов

специальность: 6М070400 - Вычислительная техника и программное обеспечение

Магистрант Ковалевский Сергей Юрьевич

_____ Ковалевский С. Ю.

Научный руководитель,

к. т. н., доцент _____Сатимова Е.Г.

АЛМАТЫ, 2014

АННОТАЦИЯ
к магистерской диссертации

Магистерской диссертации авторы: Ковалевский Сергей Юрьевич
Ғылыми бастық: к. э. н., Сатимова доцент Елена Григорьевна
Тақырып: виртуализации технологиясының
артықшылықтары ара үдеріс студенттің тәлім-тәрбиесінің.

Бұл магистрлік диссертацияның тақырыбы өзекті. Себебі, қазір әлемде студенттерді оқыту мәселесі, проблемасы ЖОО оқытушылары мен қызметкерлері алдында жиі қойылуда. Теориялық білім беру қажеттілігінен басқа, қажетті салалық білімдерді беру үшін, оқытушылар жаңа шешімдер алуы қажет. Көбіне қалыптасқан жағдайларда зертханалық жұмыстардың жүргізу онша тиімді әдіс болып табылмайды. Оқытушы қызметі тұрғысынан да, виртуалдық технологиясы жағынан да тиімді болады.

Қазіргі технологияның қолдауы арқылы оқыту тиімділігінің жақсартуын таңдау, IT мамандарының дайындауымен айналысатын компанияның виртуалдық технологиясы, эксперименттік нәтижелері негізінде іске асырылады.

Автор магистерской диссертации: Ковалевский Сергей Юрьевич

Научный руководитель: к. э. н., доцент Сатимова Елена Григорьевна

Тема: Преимущества технологии виртуализации в процессе обучения студентов.

Тема данной магистерской диссертации актуальна, поскольку, в наше время, вопрос о качественном обучении студентов встает очень часто перед преподавателями, особенно предоставление практических знаний.

Данная работа посвящена обоснованию эффективности применения технологии виртуализации, как с точки зрения преподавательской деятельности, так и эффективности самой технологии. Выбор подхода к описанию эффективности применения технологии осуществляется на основании результатов экспериментального внедрения технологии виртуализации в компанию, занимающуюся подготовкой IT специалистов.

Copyright master's thesis: Sergey Kovalevsky

Supervisor: qem. n., Associate Professor Satimov Elena G.

Topic: Benefits of virtualization technology in the learning process of students

The theme of this master's thesis is relevant because, in the modern world , the issue of quality teaching students very often gets in front of faculty and staff of universities . In addition to the necessary theoretical knowledge, to provide the necessary practical knowledge.

This work is devoted to the justification of the effectiveness of virtualization technology, both in terms of teaching and the effectiveness of the technology itself. The approach to the description of the effectiveness of technology on the basis of the pilot implementation of virtualization technology in company engaged in the preparation of IT professionals.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ

ИТ или IT – Информационная технология или Information Technologies
ВМ – Виртуальная машина
ОС или OS – Операционная Система или Operation System
SCSI – Small computer system interface
ПК или PC – Персональный Компьютер или Personal Computer
MB – Mega Bite
GB – Giga Bite
RAM – Random Access Memory
HDD – Hard Disk Device
СУБД – Система Управления Базами Данных
БД – База Данных
SC – Shared Cache
DA – Direct Access
App-V – associative parallel processor-virtualized
АД или AD – Актив Директори или Active Directory
MDOP – Microsoft Desktop Optimization Pack
SSL – Secure Socket Layer
TLS – Transport Layer Security
CA – certificate authority

ВВЕДЕНИЕ

В условиях современных технологий и скорости их развития далеко не всегда удается угнаться за техническим прогрессом, особенно это касается IT технологий. К сожалению очень часто получается именно так что после того как нам удается освоить одну технологию затратив ее изучение огромное количество времени и сил, ей на смену приходит другая – более современная, далеко не всегда, быстро-осваиваемая, но необходимая к изучению. И, к сожалению, в условиях учебного заведения далеко не все технические дисциплины возможно освоить, без возможности «пощупать» тот или иной принцип в действии.

Так, например, ни один институт нашего города Алматы не выпускает технических специалистов в области администрирования серверов или серверных систем. Конечно же, институт дает все необходимые теоретические знания, но вот практическими знаниями приходиться запасаться уже, будучи системным администратором и работая в какой-либо компании. И вот, столкнувшись с той или иной проблемой, затрачивается огромное количество времени на ее решение. Понимая, что физически невозможно - на занятиях предоставить каждому студенту свой собственный сервер для обучения работы на нем и после одной учебной пары занятий предоставить в таком же рабочем состоянии эти же или другие сервера для следующей группы, в некоторых предприятиях стали использовать технологию виртуализации. В данной диссертационной работе рассмотрены способы применения, различные виды виртуализации и преимущества данной технологии. Более детально рассмотрена технология VMware и Hyper-v.

1 Обзор технологии виртуализации

Виртуализацией в ИТ называют процесс изоляции компьютерных ресурсов друг от друга, позволяющий уменьшить зависимости между ними. Это упрощает управление изменениями в системе за счет их локализации в том или ином слое изолированных с помощью виртуализации ресурсов.

В физической среде аппаратное обеспечение, операционная система и программы тесно связаны и сильно зависят друг от друга. В виртуализированной среде, наоборот, виртуализированные элементы логически изолированы и зависят друг от друга значительно меньше.

Чтобы лучше понять, как это происходит, рассмотрим широко применяемый принцип «машинной виртуализации». На хост-компьютере устанавливается программный комплекс — гипервизор виртуальных машин, осуществляющий разделение ресурсов системы: оперативной памяти, процессора и устройств ввода-вывода между виртуальными машинами. Каждая виртуальная машина (ВМ) эмулирует обычный физический компьютер, и соответственно на ней может быть развернута операционная система и приложения. При этом машинная виртуализация обеспечивает такую степень изолированности и надежности, как если бы каждая виртуальная машина работала независимо на своем собственном оборудовании.

Виртуальную машину можно легко останавливать, делать резервные копии и запускать заново, оперируя набором файлов, описывающих текущее состояние ее оперативной памяти и жесткого диска. Так как в виртуальной машине эмулируется виртуальное оборудование, универсальное для всех хост-систем, виртуальные машины можно переносить на другие компьютеры, даже если аппаратная конфигурация этих систем не совпадает.

1.1 История развития виртуализации

Всё начиналось с виртуализации памяти на машинах второго поколения в качестве средства расширения размеров оперативной памяти. Потребность в механизме расширения возникла из-за того, что использовавшаяся в то время память на ферритовых сердечниках стоила чрезвычайно дорого. Поэтому казалось логичным виртуализовать ее, то есть расширить за счет использования внешних устройств.

Впервые виртуальная машина появилась в 1961 году в супервизоре суперкомпьютера Atlas, который был разработан английской компанией Ferranti. В середине 60-х годов она была реализована в проект IBM M44/44X Project и машине IBM 7044.

Следующим шагом в развитии идеи виртуализации стала концепция «виртуальной машины». Она появилась в 1965 году, когда исследователи в корпорации IBM предприняли экспериментальную попытку разделить компьютер на отдельные небольшие части. Это направление исследований привело к созданию многопользовательской операционной среды на

машинах IBM System 370 и System 390 и операционной системы VM/ESA, совместно называемых генеалогической линией IBM VM (Virtual Machine).

Проект СВМ/Система Виртуальных Машин являлся частью комплексной программы ЕС ЭВМ (аналога IBM System/370), которая была начата в 1969 году. Адаптация системы IBM VM/370 Release 5 и программных продуктов ее окружения были основными целями в начале проекта СВМ.

СВМ (VM, и её ранняя версия CP/CMS) — первая система, в которой была реализована технология виртуальных машин. Виртуализация в СВМ была последовательной и полной, в частности, на виртуальной машине можно было запустить другую копию системы СВМ, и так далее.

Архитектурно СВМ состояла из нескольких независимых компонентов. Центральным компонентом был монитор виртуальных машин (МВМ, IBM-овское название — CP, Control Program), который управлял аппаратурой реальной ЭВМ и реализовывал набор виртуальных машин с заданной конфигурацией. Остальные компоненты представляли собой операционные системы или системонезависимые программы виртуальных машин, работавшие под управлением МВМ: подсистема диалоговой обработки (ПДО), подсистема сетевой передачи файлов (ПСП), подсистема логической коммутации абонентских пунктов (ПЛК), подсистема анализа дампов (ПАД), подсистема дистанционной передачи файлов (ПДП), подсистема контроля технических средств (ПКТ), средства генерации и обслуживания (СГО).

Фирма VMWare первой в 1998 году реализовала на архитектуре x86 свою патентованную технологию полной виртуализации, основанную частично на бинарной трансляции и частично на выполнении инструкций прямо на физическом процессоре. Перед выполнением гостевой код просматривается на предмет проблемных инструкций, в спорных местах вставляются команды перехода на гипервизор, где специальный генератор кода заменяет «плохие» инструкции набором «правильных» инструкций.

Появление возможности запускать не модифицированную ОС позволило виртуализировать не только ОС Linux/UNIX, но и Windows.

1.2 Виды виртуализации

1.2.1Виртуализация платформ

В наше время, под виртуализацией платформы принято понимать - создание программных систем в основе существующих аппаратно программных комплексов, которые зависят или не зависят от них. Система, предоставляющая аппаратные ресурсы, а также программное обеспечение (Рисунок 1), называется хостовой, а симулируемые ею системы – гостевыми. Для того, чтобы гостевые системы могли стабильно функционировать на платформах хостовой системы, необходимо чтобы аппаратное и программное обеспечение хоста было весьма надежным, а также чтобы предоставляло необходимый набор интерфейсов доступа к ресурсам. Есть

несколько видов платформ виртуализации, в каждом из них осуществляется свой подход к понятию - виртуализация. Виды виртуализации платформ зависят от того, насколько полно осуществляется симуляция аппаратного обеспечения. До сих пор нет единого соглашения в терминах в сфере виртуализации, поэтому некоторые из приведенных ниже видов виртуализации могут отличаться от тех, что предоставят другие источники.

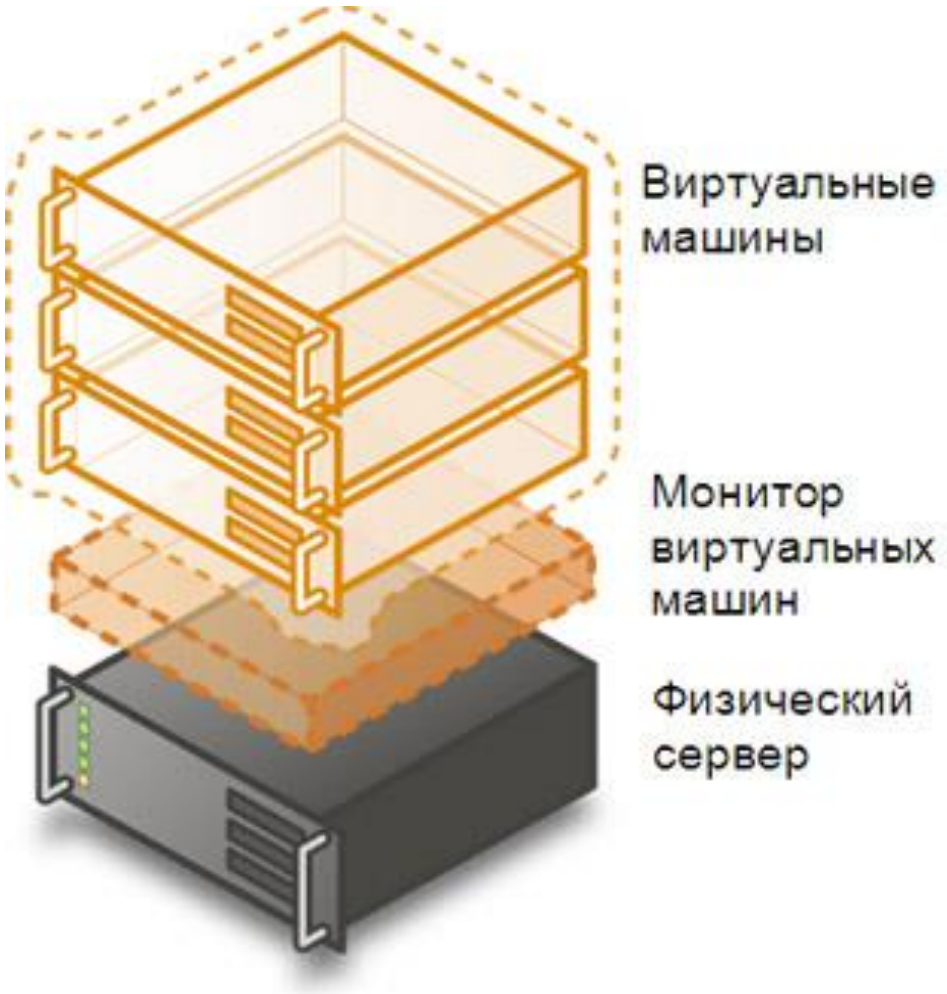


Рисунок 1 – Виртуализация платформ

1.2.2 Частичная эмуляция (нативная виртуализация)

Виртуальная машина виртуализует лишь то необходимое количество аппаратного обеспечения (оперативной памяти, памяти на жёстком диске и прочее) для того, чтобы она могла быть запущена именно изолированно. Такой подход позволяет запускать гостевые операционные системы, разработанные только для той же архитектуры, что и у хоста. Таким образом, несколько экземпляров гостевых систем могут запуститься одновременно. Этот тип виртуализации позволяет существенно увеличить быстродействие гостевых систем по сравнению с полной эмуляцией и широко используется в настоящее время. Также, в целях повышения быстродействия и качества в работе (стабильности), в платформах виртуализации, использующих данный

подход, применяется специальный слой между гостевой операционной системами и оборудованием т.е. технология - гипервизор, позволяющая гостевой системе напрямую обращаться к ресурсам аппаратного обеспечения. Гипервизор, называемый иногда - Монитор виртуальных машин (Virtual Machine Monitor) - одно из ключевых понятий в технологии виртуализации. Применение гипервизора, являющегося связующим звеном между гостевыми системами и аппаратурой, существенно увеличивает быстродействие платформы, таким образом, приближая его к быстродействию физической платформы (Рисунок 2).

Рисунок 2 – Нативная виртуализация

К минусам данного вида виртуализации можно отностся зависимость виртуальных машин от архитектуры аппаратной платформы.

Примеры продуктов для нативной виртуализации: Virtual PC, VMware Workstation, VMware ESX Server, Virtual Iron, VirtualBox, VMware Server, Parallels Desktop и прочие.

Полная эмуляция

При таком виде виртуализации, виртуальная машина полностью виртуализирует все свое аппаратное обеспечение при сохранении гостевой операционной системы в неизменном виде. Такой подход позволяет эмулировать различные аппаратные архитектуры, какие бы нам не были необходимы. К примеру, можно запускать виртуальные машины с гостевыми системами для x86-процессоров на платформах используя другую архитектурой, например, на RISC-серверах компании Sun. Ранее такой вид виртуализации использовался для разрабатывания программного обеспечения, для новых процессоров еще до того, как они были физически доступны. Такие эмуляторы также применяют для низкоуровневой отладки операционных систем. Основной минус подхода заключается в том, что эмулируемое аппаратное обеспечение весьма и весьма существенно замедляет быстродействие гостевой системы, что делает работу очень

неудобной, поэтому, кроме как для разработки системного программного обеспечения, а также образовательных целей, такой подход мало где используется (Рисунок 3).

Примеры продуктов для создания эмуляторов: Bochs, PearPC, QEMU (без ускорения), Hercules Emulator.

Рисунок 3 – Полная эмуляция

Частичная виртуализация, а также «виртуализация адресного пространства»

При таком подходе, виртуальная машина симулирует сразу несколько экземпляров аппаратного окружения, в частности даже пространства адресов. Такой тип виртуализации позволяет совместно использовать ресурсы, а также изолировать процессы, однако не позволяет разделять экземпляры гостевых операционных систем. По-другому говоря, при таком виде виртуализации пользователем не создаются виртуальные машины и происходит изоляция каких-либо процессов на уровне операционной системы, что иногда очень удобно. В наше время, очень многие из известных операционных систем используют такой подход. Примером может послужить использование технологии UML (User-mode Linux), в которой гостевое ядро запускается в пользовательском пространстве базового ядра, т.е. в его контексте (Рисунок 4).

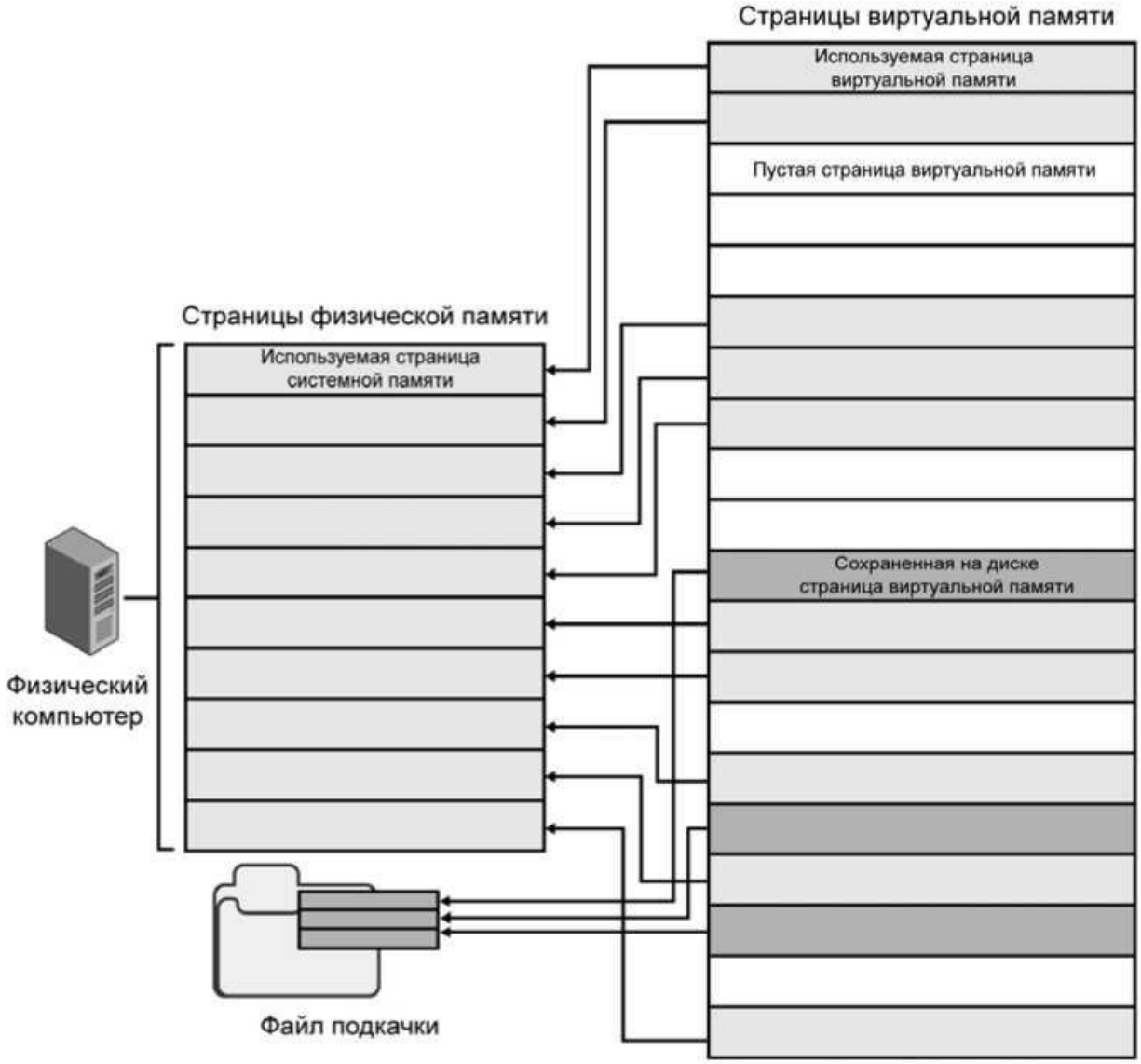


Рисунок 4 – Частичная виртуализация

Виртуализация уровня операционной системы

Сутью данного вида виртуализации является виртуализация физического сервера на уровне операционной системы в целях создания нескольких защищенных виртуализованных серверов на одном физическом. Гостевая система, в данном случае, разделяет использование одного ядра хостовой операционной системы с другими гостевыми системами. Виртуальная машина представляет собой окружение для приложений, запускаемых изолированно. Данный тип виртуализации применяется при организации систем хостинга, когда в рамках одного экземпляра ядра требуется поддерживать несколько виртуальных серверов клиентов.

Примеры виртуализации уровня ОС: Linux-VServer, Virtuozzo, OpenVZ, Solaris Containers и FreeBSD Jails.

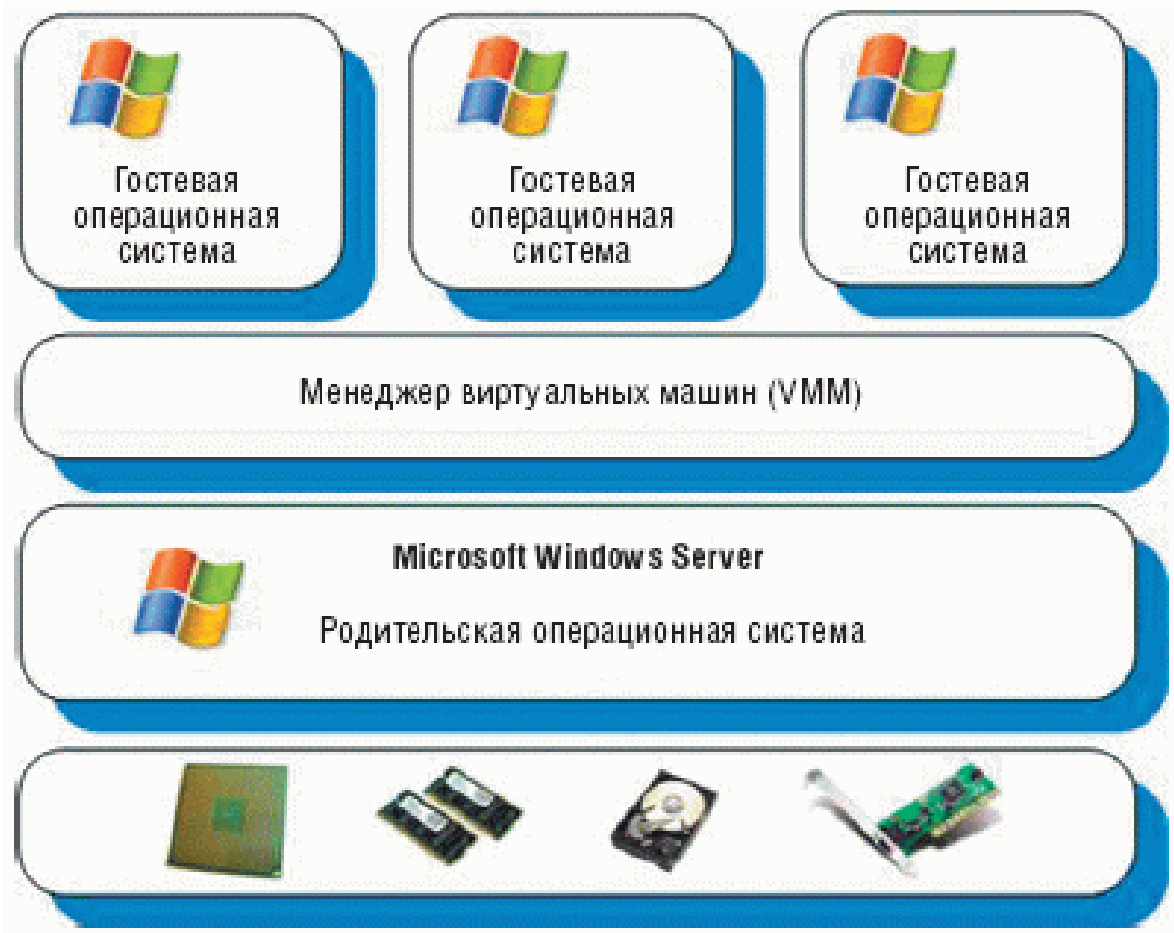


Рисунок 5 - Виртуализация уровня операционной системы

Паравиртуализация

При применении паравиртуализации нет необходимости симулировать аппаратное обеспечение, так как, вместо этого или в дополнение к этому, используется специальный программный интерфейс называемый – API, для взаимодействия с гостевой операционной системой. Данный подход требует модификации кода гостевой системы, что с точки зрения такого сообщества как Open Source не так уж и критично. Системы для паравиртуализации также имеют свой собственный гипервизор, а API-вызовы к гостевой системе, называются «hypercalls» (гипервызовы). Многие сомневаются в перспективах такого подхода к виртуализации, поскольку в данный момент все решения производителей аппаратного обеспечения в отношении виртуализации направлены на системы с нативной виртуализацией, а также, поддержку паравиртуализации приходиться искать у производителей операционных систем, которые слабо верят в возможности предлагаемого им средства. В наше время провайдерами паравиртуализации являются компании Virtual Iron и XenSource, которые утверждают, что быстродействие паравиртуализации выше (Рисунок 6).

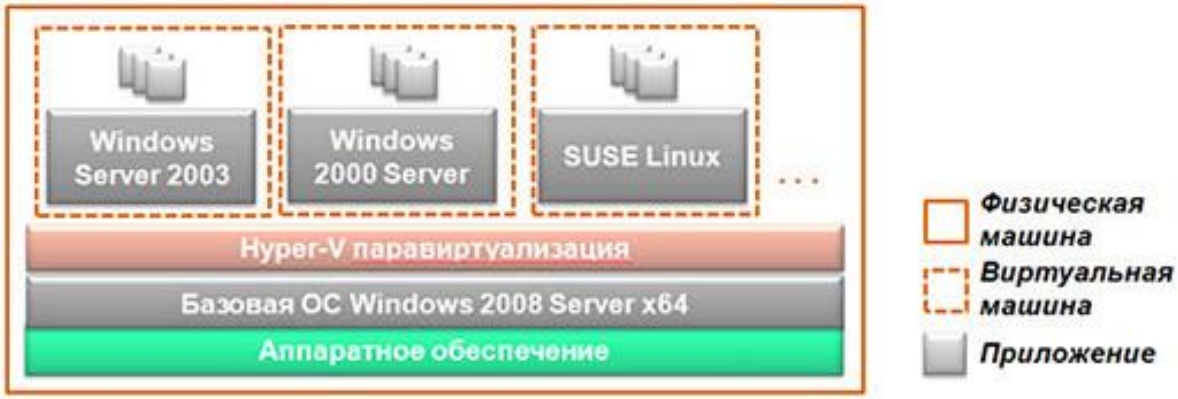


Рисунок 6 - Паравиртуализация

Виртуализация уровня приложений

Этот вид виртуализации не похож на все остальные: если в предыдущих случаях создаются виртуальные среды или виртуальные машины, использующиеся для изоляции приложений, то в данном случае само приложение помещается в контейнер с необходимыми элементами для своей работы: файлами реестра, конфигурационными файлами, пользовательскими и системными объектами. В результате получается приложение, не требующее установки на аналогичной платформе. При переносе такого приложения на другую машину и его запуске, виртуальное окружение, созданное для программы, разрешает конфликты между ней и операционной системой, а также другими приложениями (Рисунок 7). Такой способ виртуализации похож на поведение интерпретаторов различных языков программирования (не даром интерпретатор, Виртуальная Машина Java (JVM), тоже попадает в эту категорию).

Примером такого подхода служат: Thinstall, Altiris, Trigence, Softricity.

Рисунок 7 – Виртуализация приложений

Виртуализация ресурсов

При описании виртуализации платформ рассматривается понятие виртуализации в узком смысле, преимущественно применяя его к процессу создания виртуальных машин. Однако, рассматривая виртуализацию в широком смысле, можно прийти к понятию виртуализации ресурсов, обобщающим в себе подходы, в создании виртуальных систем (Рисунок 8). Виртуализация ресурсов концентрирует, абстрагирует и упрощает управление группами ресурсов, таких как хранилища данных, сети и пространства имен.

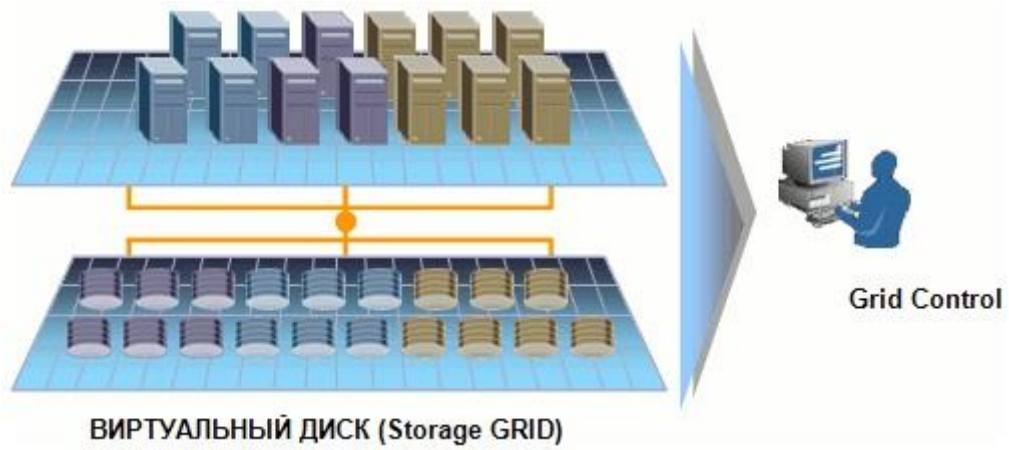


Рисунок 8 - Виртуализация ресурсов

Кластеризация компьютеров, распределенные вычисления

Этот вид виртуализации включает в себя техники, которые применяются при объединении множества отдельных компьютеров в глобальные системы (метакомпьютеры или ОСПК), решающие совместно общую задачу. Как правило примером является использование данной технологии для метеологических компаний для проведения расчетов (Рисунок 9).

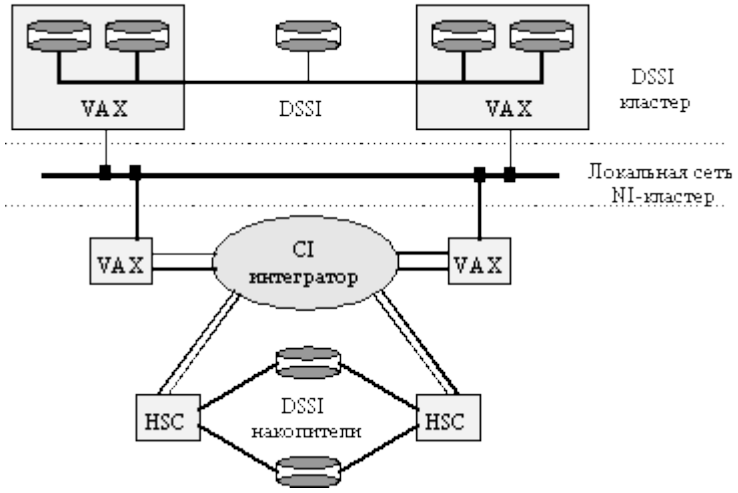


Рисунок 9 – Кластеризация компьютеров

Объединение, агрегация и концентрация компонентов

Под такими видами виртуализации, т.е. ресурсов принято понимать организацию нескольких физических или логических объектов в пулы ресурсов, т.е. группы, представляющих удобные интерфейсы для пользователя. Примеры такой виртуализации:

— многопроцессорные системы, представляющиеся как одна мощная система;

— RAID-массивы, средства управления томами, которые комбинируют несколько физических дисков в один, целый, логический;

— виртуализация систем хранения, которая используется при

построении сетей хранения данных типа SAN (Storage Area Network);

— виртуальные частные сети и трансляция сетевых адресов, позволяющие создавать виртуальные пространства, сетевых адресов, а также имен.

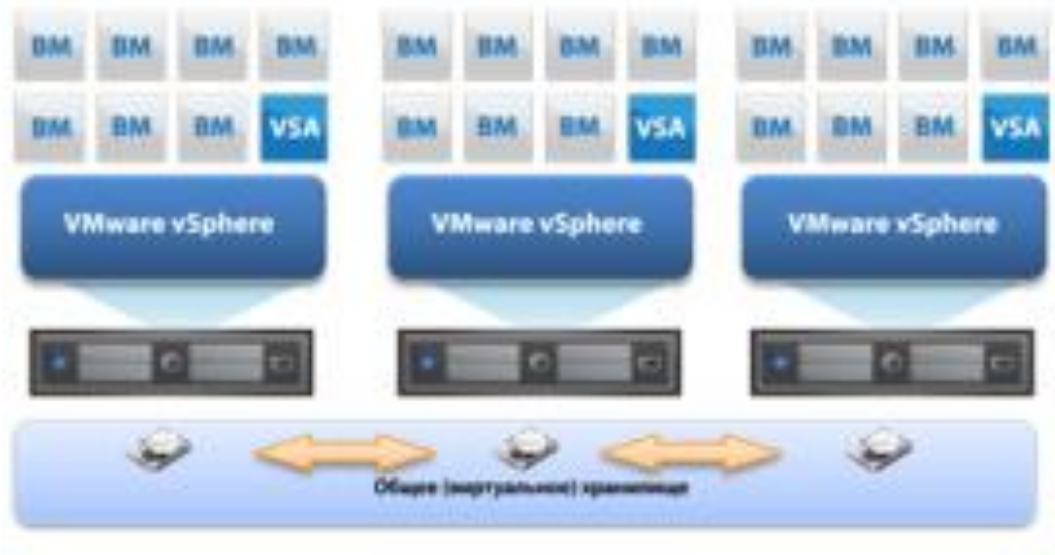


Рисунок 10 - виртуализация систем хранения

Инкапсуляция

Многим это слово известно, обычно в программировании, как сокрытие объектом внутри себя своей реализации. Применительно к виртуализации, это процесс создания системы, предоставляющей пользователю удобный для работы интерфейс и скрывающей подробности сложности своей реализации. Например, использование в ЦП кэша для организации более быстрых вычислений не отражается на его внешних интерфейсах.

Виртуализация ресурсов, в отличие от виртуализации платформ, имеет более широкий и расплывчатый смысл и представляет собой массу различных подходов, направленных на повышение удобства обращения пользователей с различными системами в целом (Рисунок 11). Поэтому, далее мы будем опираться в основном на понятие виртуализации платформ, поскольку технологии связанные именно с этим понятием являются в наше время наиболее динамично развивающимися и эффективными в использовании.

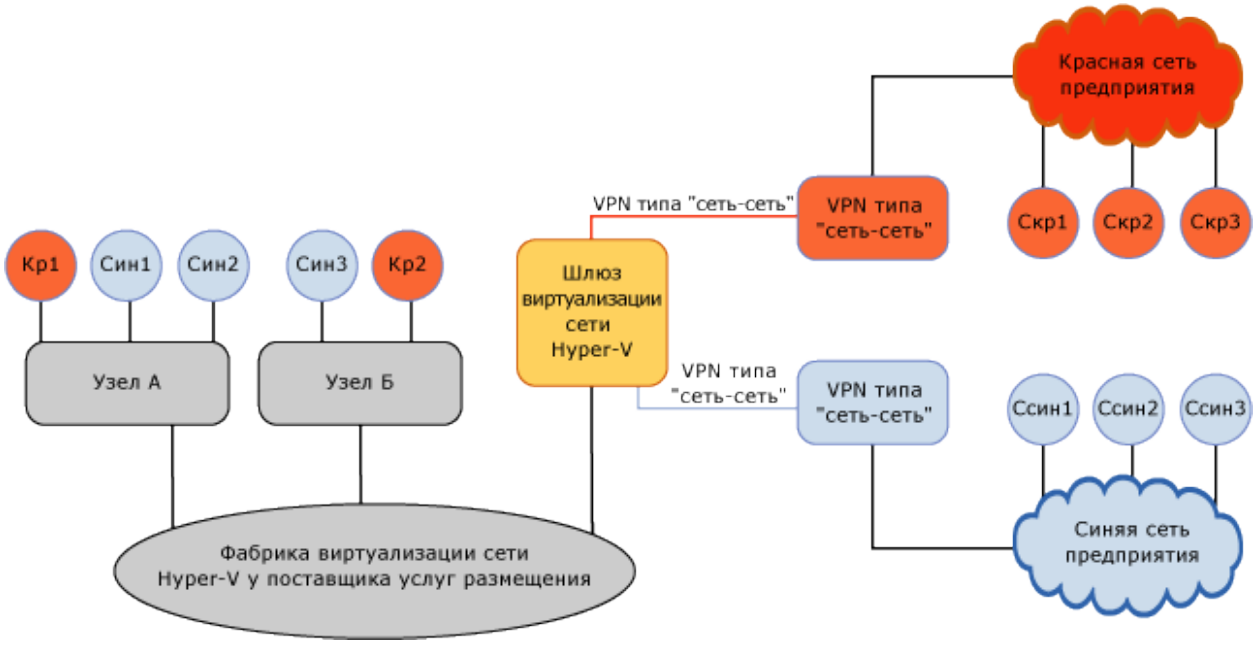


Рисунок 11 – Шлюз виртуализации сетей Hyper-V

Разделение ресурсов

При разделении ресурсов в процессе виртуализации, как правило, происходит разделение какого-нибудь одного очень большого ресурса на несколько однотипных объектов, удобных для использования. В сетях хранения данных это принято называеть зонированием ресурсов.

1.3 Преимущества виртуализации

Экономия на аппаратном обеспечении

Существенная экономия на приобретении аппаратного обеспечения происходит при размещении нескольких виртуальных серверов на одном физическом сервере (Рисунок 12). В зависимости, от поставщика платформы виртуализации, доступны возможности по настройке рабочей нагрузки, контролю выделяемых ресурсов, миграции между физическими хостами и, что самое главное, созданию бэкапа. Все это влечет за собой реальную экономию денежных средств на обслуживании, управлении, а также администрировании инфраструктуры серверов.

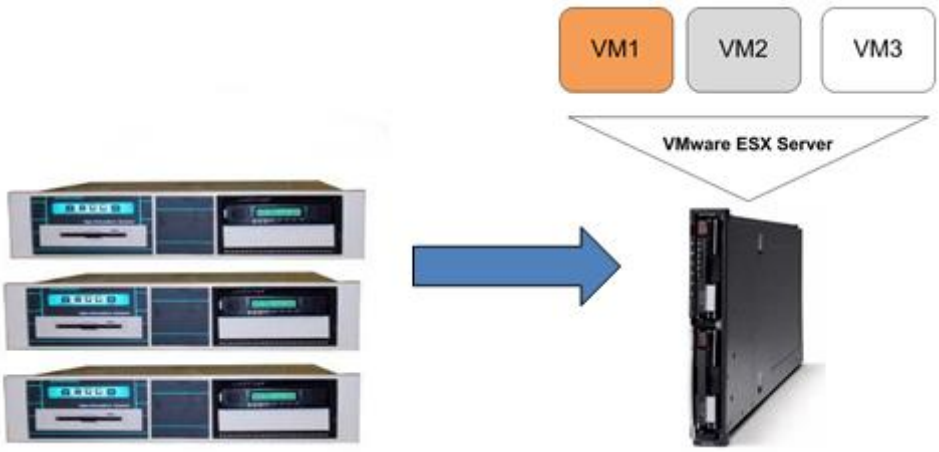


Рисунок 12 – Замена 3х серверов одним посредством VMware

Возможность поддержания старых операционных систем в целях обеспечения совместимости

При выходе новой версии операционной системы, старую версию можно запустить и поддерживать на виртуальной машине, пока не будет полностью обкатана новая ОС. И наоборот, можно «поднять» новую ОС на виртуальной машине и опробовать ее без риска для основной системы.

Возможность изолировать потенциально опасные окружения

Если какое-то приложение или компонент вызывает сомнения в его надежности и защищенности, можно использовать его на виртуальной машине без опасности повредить важные компоненты системы. Такую изолированную среду называют как правило песочницей или sandbox. Помимо этого, можно создавать виртуальные машины, ограниченные определенными политиками безопасности (к примеру, компьютер или сервер перестанет запускаться через неделю).

Возможность создания требуемых аппаратных конфигураций

Иногда требуется использовать определенную, заданную аппаратную конфигурацию (например - дисковую память, процессорное время, или количество выделяемой оперативной памяти) при проверке на работоспособность приложений в определенных условиях. Практически не реально без виртуальной машины запустить физическую машину в такие условия. В виртуальных машинах – это несколько секунд или пара кликов мыши.

Представления устройств, которых нет

К примеру, очень многие системы виртуализации позволяют создавать виртуальные SCSI диски (диски с более высокой скоростью обмена информации, которые в свою очередь стоят не дешево), виртуальные многоядерные процессоры и т.п. Это, как правило, необходимо для создания разного рода симуляций.

На одном хосте может быть запущено несколько виртуальных машин, которые объединены в виртуальную сеть

Такая особенность предоставляет безграничные возможности по созданию моделей виртуальной сети между несколькими компьютерами и серверами на одном физическом сервере. Особенно это очень необходимо, когда требуется смоделировать некую распределенную систему, которая состоит из нескольких машин. Также можно сконструировать несколько изолированных пользовательских окружений (для работы, работы в интернете или для развлечений), запустить их всех одновременно и переключаться между ними по мере необходимости выполнения различных задач.

Возможности по обучению работе с операционными системами

Можно создать репозиторий готовых к использованию виртуальных машин с различными гостевыми операционными системами и запускать их, для различных студентов (для каждого свой сервер или своя ОС), по мере необходимости в целях обучения. Их можно без опасения подвергать различным экспериментам, ведь их очень легко и быстро восстановить.

Виртуальные машины мобильны

Папка с виртуальной машиной может быть перемещена на другой ПК, и там может быть сразу запущена, без длительного простоя. Не требуется создавать никаких образов для миграции (обычно на это уходит от часа и больше), и, к тому же, виртуальная машина не привязана к конкретной аппаратуре.

Виртуальные машины могут быть организованы в пакеты приложений

Вы можете создать виртуальной окружение для конкретного использования (например - машину менеджера, дизайнерскую машину, и т.д.), установив в ней все требуемое программное обеспечение, и разворачивать рабочие столы по мере необходимости.

Виртуальные машины легко управляемы

При использовании виртуальных машин существенно повышается управляемость в отношении создания резервных копий (бэкапов), создания снимков состояний виртуальных машин («снапшотов») и восстановлений после сбоев.

На этом, конечно же, не исчерпываются достоинства виртуальных машин, это лишь пища для размышления и исследования их возможностей.

1.4 Недостатки виртуализации

Невозможность эмуляции всех устройств

В данный момент все основные устройства аппаратных платформ

поддерживаются вендорами систем виртуализации, однако если вы используете, к примеру, какие-либо контроллеры или устройства, не поддерживаемые ими, придется отказаться от виртуализации такого окружения.

Виртуализация требует дополнительных аппаратных ресурсов

В настоящее время использование различных техник виртуализации позволило приблизить показатели быстродействия виртуальных машин к реальным, однако для того, чтобы физический хост смог запускать хотя бы пару виртуальных машин, требуется достаточное для них количество аппаратных ресурсов.

Некоторые платформы виртуализации требовательны к конкретному аппаратному обеспечению

К примеру, замечательная платформа компании VMware, ESX Server, была бы и вовсе замечательной, если бы не предъявляла жестких требований к аппаратному обеспечению.

Хорошие платформы виртуализации стоят хороших денег

Порой стоимость развертывания одного виртуального сервера равна стоимости еще одного физического, в определенных условиях это может оказаться нецелесообразным. К счастью, есть множество бесплатных решений, но они, в основном, ориентированы на домашнего пользователя и малый бизнес.

Несмотря на перечисленные и вполне устранимые недостатки, виртуализация продолжает набирать обороты и в ближайшие годы ожидается существенное расширение, как рынка платформ виртуализации, так и средств управления виртуальными инфраструктурами. За последние несколько лет интерес к виртуализации вырос в разы.

2 Экспериментальное внедрение технологии виртуализации в процесс обучения компании «ТОО Каисса»

В ТОО Каисса был проведен эксперимент в ходе, которого удалось выяснить и наглядно сравнить работоспособность и стабильность работы сервера с технологией виртуализации по сравнению с обычным использованием ПК.

Эксперимент проводился в двух аудиториях для подготовки специалистов в области разработки и создания базы данных в SQL, со всем необходимым программным обеспечением. В обеих аудиториях устанавливается стандартное программное обеспечение для обучения специалистов: Языки программирования, Mathcad, AutoCAD, MS Office, и прочее. Единственным отличием является именно то, что в одной аудитории устанавливается сервер, настраивается Active Directory, производится настройка домена. Далее - разворачивается VMware с 12 виртуальными машинами, на одной устанавливается SQL Server – для обучения разработчиков, по окончанию установки и настройки - снимается образ для перекидывания на остальные 11 виртуальных машин и резервного восстановления на случай непредвиденных проблем.

В другой аудитории для обучения разработчиков – на каждом компьютере устанавливается VMware, и на одной виртуальной машине устанавливается OS Linux, на котором ставится SQL Server, настраивается, после этого сохраняется образ одной виртуальной машины и ставится его на остальные 11 компьютеров.

Весь эксперимент состоит из трех частей.

Цель первой части эксперимента – подготовка учебных аудитории, т.е. установка и настройка программного обеспечения.

Цель второй части эксперимента – экспериментальная проверка работоспособности и стабильной работы двух аудиторий, а также фиксирование всех случаев технических проблем и фиксирование времени на их устранение.

Цель третьей части – подсчет и обработка всех полученных в ходе эксперимента данных и вывод.

2.1 О компании

Компания ТОО Каисса основана в 2007 году и занимается предоставлением IT аутсорсинга и разработкой программного обеспечения.

В штате компании насчитывается более ста сотрудников. Большая часть этих сотрудников – IT специалисты, системные администраторы, программисты.

В компаниях, которые занимаются подобными услугами обычно очень большая текучесть кадров, что в свою очередь означает, что очень часто приходится сталкиваться с новыми сотрудниками. Поскольку компании не выгодно нанимать опытных специалистов, т.к. руководство не устраивает требования по заработной плате опытных специалистов, компания занимается обучением и повышением квалификации своих собственных сотрудников. Особое внимание уделяется обучению новеньких – стажеров, т.к. чем быстрее они обучаться, тем быстрее вольются в работу общего коллектива. В компании имеется две учебные аудитории. Одна – для подготовки системных администраторов и вторая для подготовки разработчиков, в обеих аудиториях по 12 стационарных компьютеров.

2.2 Определение задач эксперимента

Целью эксперимента было определить работоспособность, стабильности работы и времени затраченного на восстановление работоспособности сервера с технологией виртуализации по сравнению с обычным использованием ПК в процессе обучения.

Для этого эксперимент проводился в двух аудиториях для подготовки специалистов в области разработки и создания базы данных в SQL, со всем необходимым программным обеспечением. В обеих аудиториях устанавливается стандартное программное обеспечение для обучения специалистов: Языки программирования, Mathcad, AutoCAD, MS Office, и прочее. Единственным отличием является именно то, что в одной аудитории устанавливается сервер, настраивается Active Directory, производится настройка домена. Далее - разворачивается VMware с 12 виртуальными машинами, на одной устанавливается SQL Server – для обучения разработчиков, по окончанию установки и настройки - снимается образ для перекидывания на остальные 11 виртуальных машин и резервного восстановления на случай непредвиденных проблем.

В другой аудитории для обучения разработчиков – на каждом компьютере устанавливается VMware, и на одной виртуальной машине устанавливается OS Linux, на котором ставится SQL Server, настраивается, после этого сохраняется образ одной виртуальной машины и ставится его на остальные 11 компьютеров.

Весь эксперимент состоит из трех частей.

Цель первой части эксперимента – подготовка учебных аудиторий, т.е. установка и настройка программного обеспечения.

Цель второй части эксперимента – экспериментальная проверка работоспособности и стабильной работы двух аудиторий, а также фиксирование всех случаев технических проблем и фиксирование времени на их устранение.

Цель третьей части – подсчет и обработка всех полученных в ходе эксперимента данных и вывод.

2.3 Настройка всего необходимого для проведения эксперимента

Количество испытуемых ПК – 24 .

Количество аудиторий – 2 по 12 ПК в каждой. (рисунок 13, рисунок 14)

Параметры ПК – OS Windows 7 x32, HDD 500Gb RAM 4Gb (3,41 доступных из-за 32х битной операционной системы).

Сеть в обеих аудиториях 100Mb (ограничена параметрами свитчей TP-LINK SF1024D).

Необходимое программное обеспечение для полноценного использования ПК разработчиками – OS Windows 7, MS office 2010, Антивирус Касперского версии 6, языки программирования – Pascal, C++, C#, VMware с установленным на нем ОС Linux Debian и SQL Server. Для оптимальной работы доменной сети выбирается сервер со следующими параметрами – CPU Core i7 3.0, RAM 12Gb HDD 500GB 7200RPM, поделенный на 2 диска. Для операционной системы и установленного программного обеспечения - 320GB и 100GB для резервных образов с VMware, драйвера и дистрибутивы программ необходимых для администрирования.

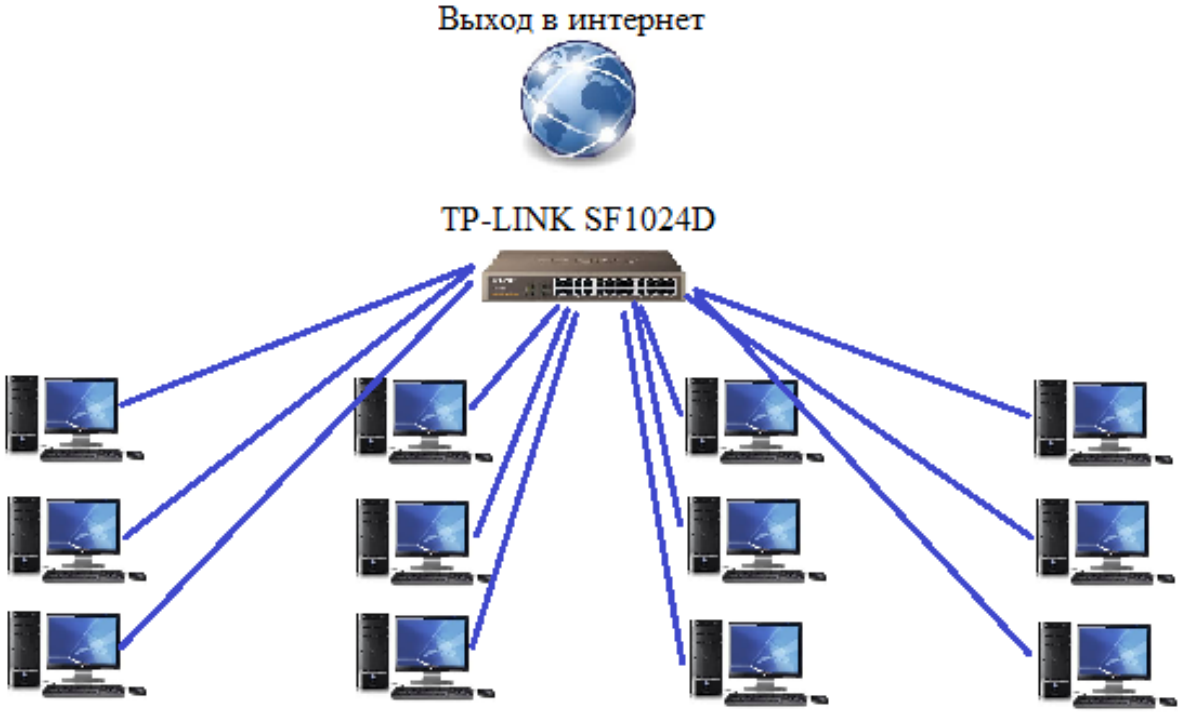


Рисунок 13 – схема аудитории «А» обычная сеть, VMware и SQL Server установлен на каждом стационарном ПК

В качестве операционной системы на сервере в аудитории «Б» (рисунок 2) выбирается Windows Server 2008, он более удобен в администрировании, чем Windows Server 2012 и более функционален в плане администрирования доменных сетей, чем предшествующие версии серверных операционных систем семейства Windows.

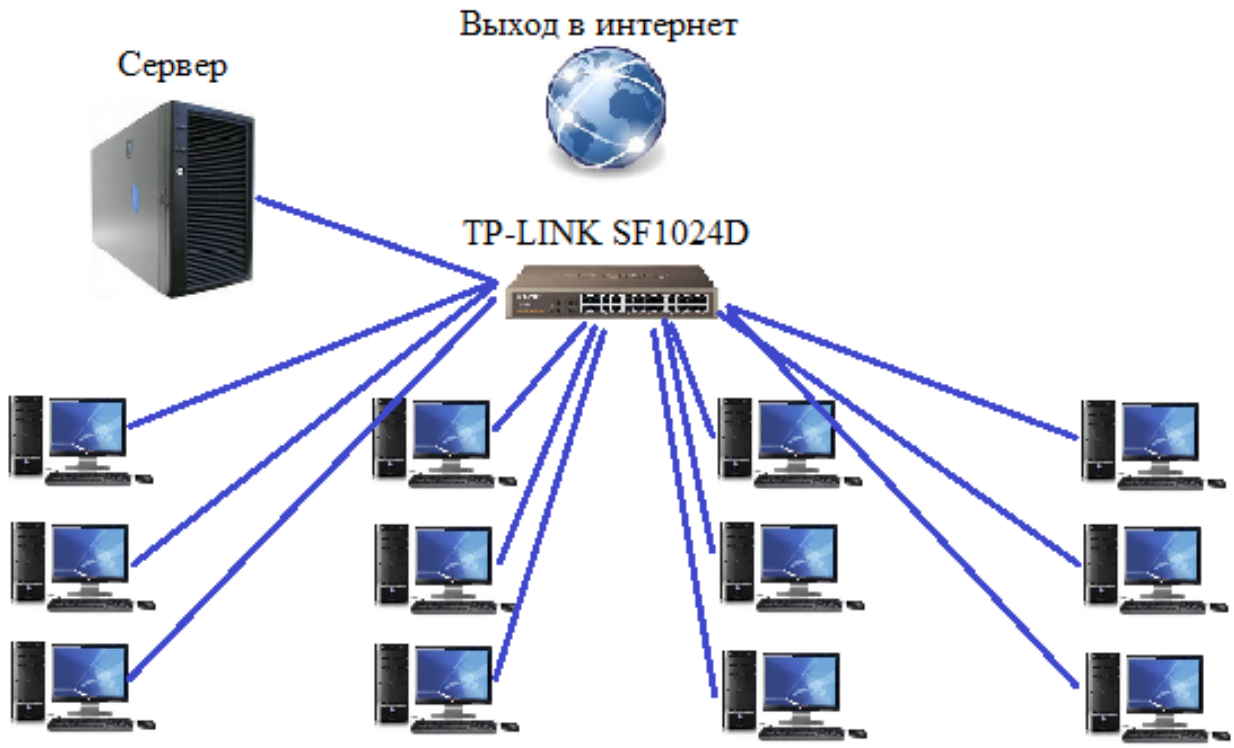


Рисунок 14 – схема аудитории «Б» доменная сеть,
VMware установлен только на сервере

Для аудитории «Б» отличиями после установки всего программного обеспечения является то, что нам не нужно устанавливать VMware с ОС Linux и SQL Server ни на один ПК кроме сервера и, вместо рабочей группы вводится ПК в единый домен с сервером. Было принято решение использовать доменную сеть по причине, возможности удобного администрирования и создание единых правил для доменной группы «студенты». Благодаря доменной архитектуре – есть возможность ограничить для обучаемого доступ на сервер, и разрешить только к выделенному для него виртуальным пространству, т.е. полностью запретить ему доступ к файлам с резервными образами и к операционной системе сервера.

Также, благодаря настроенному Active Directory, осуществляется мониторинг и логирование изменений каждого обучаемого для последующего выявления уязвимостей и их устранения (опираясь на опыт что некоторые умные ребята «способны немного пошалить»).

2.4 Установка и настройка сервера

После того как устанавливается операционная система Windows Server 2008 R2, устанавливается антивирус, был выбран антивирус Kaspersky 9.0.0.736 и первым делом настраивается на нем парольная защита на изменение настроек и отключение. В ролях сервера подключается и

настраивается Active Directory, добавляются пользователи учетные записи для домена такие как - «Студент 1», «Студент 2», … , «Студент 12», для того, чтобы у каждого обучаемого был свой доступ к серверу, под своей учетной записью. Далее устанавливается VMware с ОС Linux, SQL Server и настраивается для каждого сотрудника виртуальный SQL Server. В качестве резерва - под учетной записью администратора, на сервере поднимается еще одну (13ю VMware), но доступ на нее для всех кроме преподавателя и администратора закрывается из соображений политики безопасности (рисунок 15).

Таким образом, в сети аудитории «Б» имеется всего 13 компьютеров включая сервер, но после подключения каждого ПК к серверу для работы с SQL, обучаемый работает исключительно на своем SQL сервере.

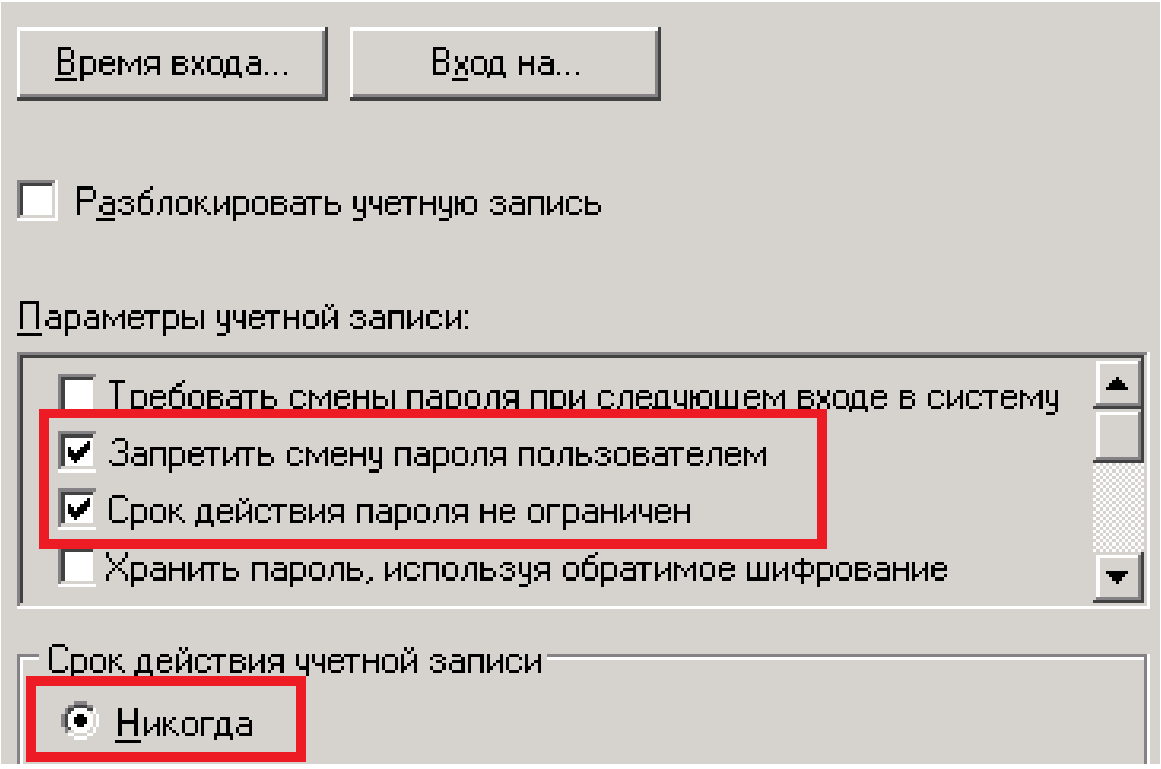


Рисунок 15 настройка пароля для студента Active Directory

Недостаток такого метода заключается в необходимости использовать довольно «мощный» сервер, который в свою очередь стоит дороже, чем обычный ПК. Однако плюсами данной технологии является – разгрузка сети, т.к. благодаря Active Directory настраивается доступ на сервер и имеется возможность запретить какое либо выявление данных виртуальных ПК с ОС Linux и SQL Server в общей сети. Самым главным плюсом является управляемость, мониторинг активности пользователей и настройка потребляемых ресурсов для VMware для всех пользователей так например для каждого обучаемого сотрудника мы на сервере выделяем по 512 MB АЗУ и 5GB места на сервере. Для самого сервера остается при максимальной нагрузке 6GB АЗУ и 260GB дискового пространства, чего более чем

достаточно для администрирования по CPU при одновременном сеансе – 12 пользователей, идет нагрузка в 30-40%, что тоже вполне допустимо.

2.5 Обработка результатов эксперимента

По истечении 4х месяцев выявлено 36 зафиксированных проблем (рисунок 16) в аудитории «А» и 12 технических проблем в аудитории «Б» (рисунок 17).

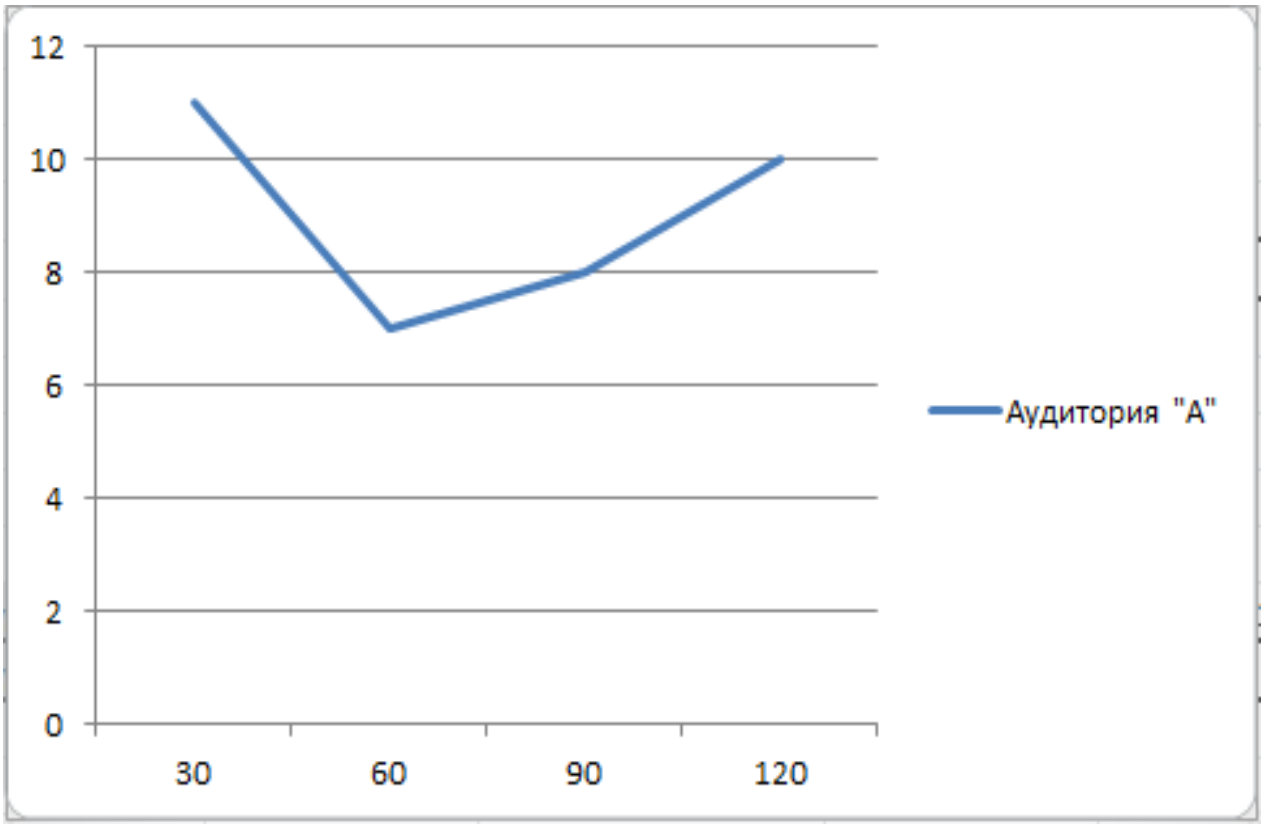


Рисунок 16 график технических проблем в аудитории «А»

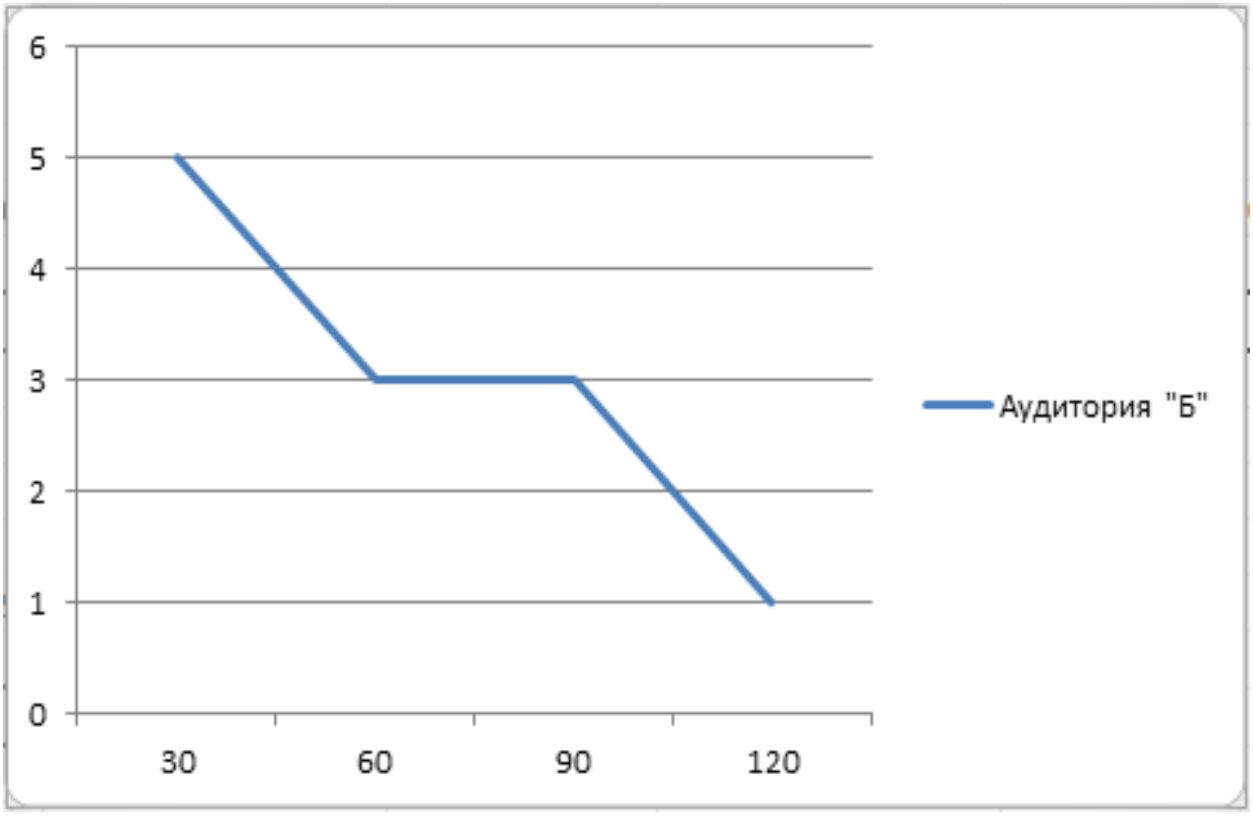


Рисунок 17 график технических проблем в аудитории «Б»

Самыми частыми проблемами в аудитории «А» являлись – слабая сеть, а также из-за большого количества виртуальных ПК свитч не успевал обрабатывать запросы и из сети часто отключались различные ПК. Так же имело место случайное удаление ПО VMware с резервным файлом – образом. Как правило, файл образ, с настроенным на нем Linux и SQL Server, имеет вес как минимум в 4,4GB. Следовательно, перекидывание этого файла по сети или через USB накопитель на ПК, где он пропал, занимает около 40 минут, а установка и настройка VMware с Linux и SQL Server не меньше 2х часов.

Самыми частыми проблемами в аудитории «Б» оказались – сложность настройки политики безопасности и некоторая специфика в администрировании ролей, прав доступа. Очень много времени на первое время уходило на осваивание принципов администрирования. Однако, после того как удалось освоить администрирование VMware, количество технических сбоев сократилось до 1 в месяц и затраченное время на устранение технических проблем также удалось сократить (таблица 4.1).

Таблица 4.1- аудиторий «А» и «Б», всех технических проблем и затраченного времени на их устранение за 4 месяца эксперимента

2.6 Анализ обработанных результатов

Основные результаты проведенного эксперимента:

Доработанная и полностью настроенная доменная система вместе с технологией виртуализации на базе VMware позволяет в 3 раза сократить случаи технических сбоев, а время устранения этих сбоев в 5 раз.

Система проста в пользовании и понятна. Однако политики безопасности и исключений требуют тщательной и внимательной настройки.

Система Windows Server 2008 R2 с технологией виртуализации позволяет дать доступ обучаемому к своему собственному виртуальному серверу и дать полноценную возможность «пощупать», настроить, испортить и восстановить ее самостоятельно, без вреда для остальных учащихся, при неудачи при восстановлении обучаемым стажером – преподаватель или системный администратор способен восстановить работоспособность SQL Server в течении 5-10 минут (в отличии от обычного метода 40 минут или более)

Технология VMware обеспечена необходимым набором функционального

обеспечения.

Т а б л и ц а 1 результат технических проблем за 4 месяца

	1й месяц		2й месяц		3й месяц		4й месяц	
	техн. Проблем (кол-во)	затрачено времени (мин)	техн. проблем (кол-во)	затрачено времени (мин)	техн. проблем (кол-во)	затрачено времени (мин)	техн. проблем (кол-во)	затрачено времени (мин)
Аудитория "А"	11	275	7	260	8	350	10	320
Аудитория "Б"	5	120	3	60	3	50	1	10

В экспериментальной части проекта участвовали сотрудники компании ТОО Каисса и обучающий персонал.

Эксперимент доказывает, что работа с Active Directory и виртуализацией позволяет каждому обучаемому индивидуально обучаться технологиям без какого – либо риска для окружающих (т.е. без вариантов срыва для остальных обучаемых). Также позволяет в среднем в 3 раза сократить риск возникновения технической проблемы, и что самое главное уменьшить время на решение возникших проблем. В заключении предлагаю для нашего института приобрести собственный кафедральный сервер, который позволит создать внутреннюю кафедральную сеть, и использовать его для дальнейшего обучения студентов, т.к. самые эффективные занятия – это те, где для студента есть возможность «потрогать» без страха, что возможно, что – то сломается.

2.7 Вывод по второй главе

В ходе данного эксперимента удалось наглядно выяснить все преимущества технологии виртуализации в процессе обучения. Огромной неожиданностью оказалось довольство именно обучающегося персонала, т.к. на вопросы типа «Точно можно удалить?» или «А что если?» они могли смело выполнять любые действия. Благодаря системе виртуализации - с легкостью восстанавливалось программное обеспечение с минимальным простоем компьютерной техники.

3 Серверная виртуализация общие понятия

Серверная виртуализация является ключевым элементом виртуализации в целом. В общем смысле серверная виртуализация это возможность виртуализировать работу серверов. Данная технология позволяет значительно сократить количество физических серверов путем их консолидации: размещение нескольких серверов на одном физическом оборудовании. Консолидация достигается путем размещения серверов в отдельных виртуальных машинах, расположенных на одном физическом сервере, и управляемых гипервизором.

Серверная виртуализация работает следующим образом - виртуальная машина представляет собой программную вычислительную среду, эмулирующую аппаратные ресурсы компьютера. Благодаря этому на одной физической машине может быть запущенно несколько операционных систем. Каждая операционная система работает в своей виртуальной среде, которой выделена определенная часть вычислительных мощностей физического компьютера. Операционная система не знает, что она запущена в виртуальной среде и ведет себя так, как будто имеет полный контроль над ресурсами физической машины.

В случае серверной виртуализации на одном физическом сервере эмулируются вычислительные среды одновременно для нескольких виртуальных серверов. Чтобы предотвратить возможные конфликты между виртуальными серверами во время использования ресурсов физической машины и для обеспечения возможности администрирования и контроля существует гипервизор

4 Технология виртуализации посредством "Гипервизор"

Гипервизор - Это программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких или даже многих операционных систем на одном и том же хост-компьютере. Гипервизор также обеспечивает изоляцию операционных систем друг от друга, защиту и безопасность, разделение ресурсов между различными запущенными ОС и управление ресурсами.

Гипервизор может предоставлять работающим под его управлением, на одном хост-компьютере, ОС средства связи и взаимодействия между собой так, как если бы эти ОС выполнялись на разных физических компьютерах.

Гипервизор сам по себе в некотором роде является минимальной операционной системой. Он предоставляет запущенным под его управлением операционным системам сервис виртуальной машины, виртуализируя или эмулируя реальное (физическое) аппаратное обеспечение конкретной машины. И управляет этими виртуальными машинами, выделением и освобождением ресурсов для них. Гипервизор позволяет независимое «включение», перезагрузку, «выключение» любой из виртуальных машин с той или иной ОС. При этом операционная система, работающая в виртуальной машине под управлением гипервизора, может, но не обязана

«знать», что она выполняется в виртуальной машине, а не на реальном аппаратном обеспечении.

Гипервизоры первого типа работают непосредственно на аппаратных ресурсах физичесого компьютера. Они функционируют как управляющая программа. Гостевые операционные системы, работающие в виртуальных машинах, располагаются уровнем выше гипервизора.

Так как гипервизоры первого типа работают неспосредственно на аппартных ресурсах компьютера они, как правило, обеспечивают наилучшее быстродействие и безопасность, чем любые дргуие типы гипервизоров.

В качестве примеров гипервизоров первого типа можно привести:

- Microsoft Hyper-V;
- Citrix XenServer;
- WMware ESX Server.

Гипервизоры второго типа работают в среде операционной системы, запущенной на физическом компьютере. Гостевые операционные системы, в свою очередь, работают в виртуальных машинах, расположенных над уровнем гипервизора.

Как видно из сравнения двух типов гипервизоров, операционные системы в виртуальных машинах, работающие под управлением гипервизора второго типа, находятся на один уровень дальше от аппаратных ресурсов физического компьютера. Этот дополнительный уровень является причиной снижения произодительности виртуальных машин гипервизоров второго типа. Кроме того, количество виртуальных машин, которые можно запустить на приемлимом уровне производительности, по той же причине значительно ограничено.

Примерами гипервизоров второго типа являются:

- Microsoft Virtual Server;
- WMware Server.

Гипервизоры с монолитной архитектурой подразумевают использование драйверов, специально написанных с учетом работы с гипервизором. Они управляются гипервизором и, по сути, выполняются в среде гипервизора.

Монолитная архитектура имеет определенные преимущества, но в то же время у нее есть довольно серьезные недостатки. Одним из основных преимуществ можно назвать отсутствие необходимости в родительской операционной системе, так как все гостевые операционные системы напрямую работают с аппаратными средствами физического компьютера посредством драйверов в гипервизоре.

С другой стороны тот факт, что драйверы должны быть специально написаны для гипервизора, создает определенные трудности. Учитывая разнообразие и количество устройств, вероятность того, что для конкретного устройства не найдется специального драйвера, довольно высока. Это ведет к необходимости тесного сотрудничества между производителями гипервизоров и аппаратных устройств, с целью обеспечить специализированные драйверы. Это в свою очередь означает, что производители гипервизоров данной архитектуры зависимы от

производителей аппаратных устройств, так как без специализированных драйверов их продукт не имеет ценности. Все это ведет к тому, что количество устройств, на которых могут работать гипервизоры данной архитектуры, как правило, меньше, чем количество устройств, на которых способны работать гипервизоры другой архитектуры.

Данная архитектура так же представляет потенциальную угрозу безопасности. Так как драйверы производителей устройств с перспективы гипервизора считаются сторонним кодом, выполнения их в гипервизоре на самом привилегированном уровне может представлять опасность.

Примером гипервизора с монолитной архитектурой является VMware ESX Server.

Гипервизоры микро ядерной архитектуры не нуждаются в специализированных драйверах, так как они имеют операционную систему, находящуюся в родительском разделе. Этот родительский раздел обеспечивает среду, в которой запускаются драйверы для аппаратных устройств физического компьютера. Раздел можно понимать как одну из виртуальных машин, запущенных на гипервизоре.

В микро ядерной архитектуре необходимо установить драйверы устройств только для операционной системы, находящейся в родительском разделе. Нет необходимости устанавливать драйверы для всех виртуальных машин, так как когда у виртуальной машины возникает необходимость получить доступ к физическому устройству компьютера, она делает это путем обращения к родительскому разделу. Другими словами в микро ядерной архитектуре у гостевых операционных систем нет возможности напрямую использовать физические ресурсы компьютера, они делают это только через запросы родительской операционной системе.

Микро ядерная архитектура имеет определенные преимущества по сравнению с монолитной. Во-первых, так как необходимости в специализированных драйверах нет, возможно использование всего спектра существующего оборудования. Во-вторых, отсутствие встроенных драйверов снимает с гипервизора дополнительную нагрузку, что делает его меньше и менее сложным, соответственно более надежным. В-третьих, отсутствие стороннего кода внутри гипервизора (которым являются драйверы), снимает риск потенциальных проблем с безопасностью.

Однако микро ядерная архитектура имеет заметный недостаток — необходимость в родительском разделе. Это добавляет дополнительную нагрузку на систему (в большинстве случаев приемлемую), в связи с необходимостью поддержания родительского раздела и осуществлением и контролем запросов дочерних разделов на физические ресурсы компьютера.

Примером гипервизора с микро ядерной архитектурой является Microsoft Hyper-V.

5. Виртуализация серверов баз данных (будет 3я глава)

Виртуализация серверов баз данных является одним из основных

направлений данной технологии. Учитывая необходимость в централизованном хранении информации, которое обеспечивают серверы с СУБД, и их наличие в организациях практически любого уровня, делают серверы баз данных наиболее очевидным претендентом на виртуализацию.

Применительно к кафедре можно выделить сразу две СУБД, как потеницальных кандидатов на виртуализацию:

- MS SQL Server;
- Oracle.

Виртуализация данных СУБД обеспечит ряд преимуществ, по сравнения с традиционной моделью развертывания СУБД.

Рассмотрим их более подробно.

5.1 Эффективное использование ресурсов

Благодаря размещению СУБД на виртуальной машине основного сервера нет необходимости в покупке отдельной физической машины для выполнения данной роли. Кроме того, с учетом небольших размеров кафедры, можно с большой долей вероятности говороить о том, что ресурсы выделенного для этой цели сервера не будут использоваться полностью. Так как применительно к кафдре таких серверов нужно два, по одному на каждую СУБД, необоснованные расходы возрастут вдвое. Расход электричесих ресурсов так-же снижается.

5.2 Упрощенное администрирование

С использованием виртуализации задачи по администрированию серверов с СУБД значительно упрощаются. Использую снимки виртуальных машин, кластеризацию и возможность переноса виртуальных машин внутри кластера позволяют создать среду, в которой время простоя будет сведено к минимуму. Кроме того, при отказе виртуального сервера с СУБД время на восстановление работы возможно минимизировать и парктически устранить проблему потери важной информации.

5.3 Динамичность IT-инфраструктуры

Использование виртуализации позволяет осуществлять динамичное перераспределение ресурсов между серверами, что позволяет всей инфраструктуре подстраиваться под нагрузку в каждый отдельный момент времени, обеспечивая таким образом комфортную работу всем пользователям.

5.4 Реализация

Рассмотрим традиционную модель развертывания СУБД. Без применения виртуализации каждую отдельную СУБД необходимо развертывать на отдельной физической машине. Это необходимо чтобы избежать возможных конфликтов между разными СУБД. В результате имеем минимум два сервера с установленными на них разными СУБД, как показано на рисунке 18.

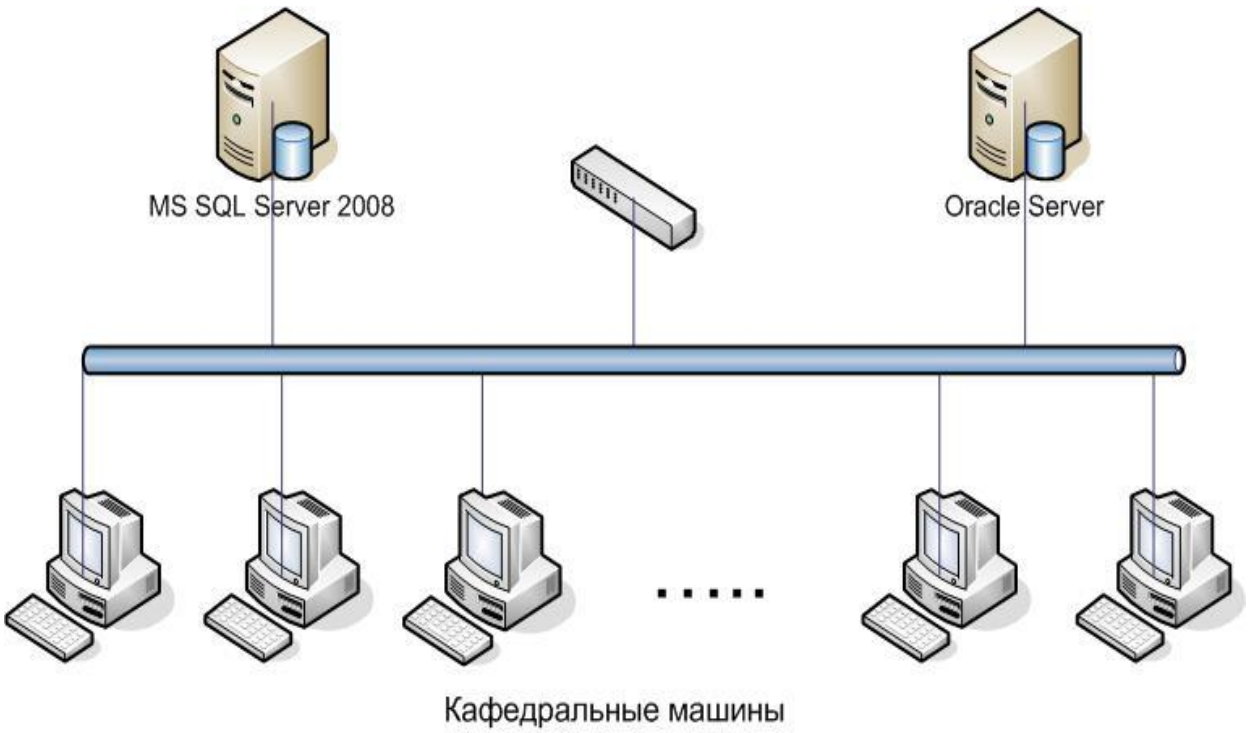


Рисунок 18 - Традиционная модель

Как видно из рисунка, в традиционной модели есть два отдельных физических сервера. Клиентские машины подключаются к сети и работают с тем сервером, который в данный момент необходим. Рассмотрим достоинства и недостатки данной модели.

Преимущество:

Простота реализации — при таком способе развертывания серверов с СУБД не требуется никаких дополнительных действий, кроме непосредственно установки и настройки СУБД на серверы.

Недостатки:

1Низкая отказоустойчивость — при выходе из строя физического оборудования сервера время простоя будет измеряться часами, если не сутками.

2Сложность резервного копирования — для резервного копирования операционных систем на случай их отказа придется использовать стороннее программное обеспечение, которое, как правило, требует дополнительных вложений.

Указанные недостатки могли бы быть решены, используя репликацию или подобные технологии от производителей СУБД, но они потребуют еще по одному серверу на каждую СУБД, что значительно увеличит стоимость системы.

Теперь посмотрим как данная системы будет выглядеть используя технологию виртуализации. В данном варианте обе СУБД располагаются на одном физическом сервере. Каждая СУБД установлена на отдельной виртуальной машине, чтобы исключить возможные конфликты, как показано

на рисунке 19.

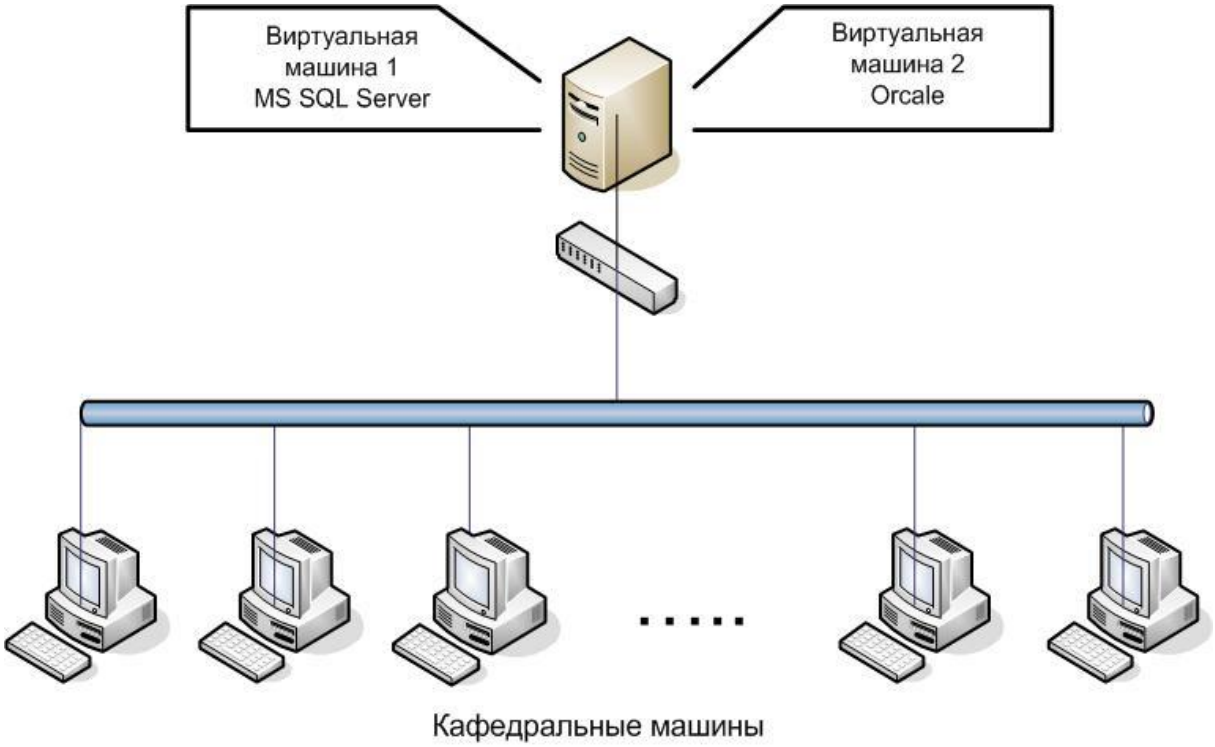


Рисунок 19 - Использование виртуализации

Как видно из рисунка, оба сервера находятся на одном физическом компьютере, но в разных виртуальных средах. Это одновременно предоставляет каждой СУБД свою «чистую» операционную систему, и сокращает количество физического оборудования. Рассмотрим достоинства и недостатки данной системы.

Преимущества:

1Использование ресурсов — при размещении обеих СУБД на одном сервере ресурсы сервера используются эффективнее, в результате чего повышается эффективность вложения средств.

2Резервное копирование и администрирование — в силу встроенных инструментов по управлению виртуальными машинами, резервное копирование становится простой задачей. Снимки виртуальных машин можно хранить отдельно на отказоустойчивом внешнем хранилище. Восстановление виртуального сервера после отказа операционной системы не займет и получаса. При этом сделать это можно удаленно.

На первый взгляд может показаться, что данная система менее надежна, так как если сервер выйдет из строя, то выйдут из строя и оба виртуальных сервера. Однако это проблема решается созданием кластера и более подробно рассмотрена в последней главе.

5.5 Процесс создания виртуального сервера

Виртуальный сервер представляет собой виртуальную машину с установленным на нее серверным программным обеспечением. Соответственно создание виртуального сервера практически ничем не отличается от создания виртуальной машины.

Создание виртуальных машин осуществляется с помощью управляющей консоли Hyper-V, как показано на рисунке 20.

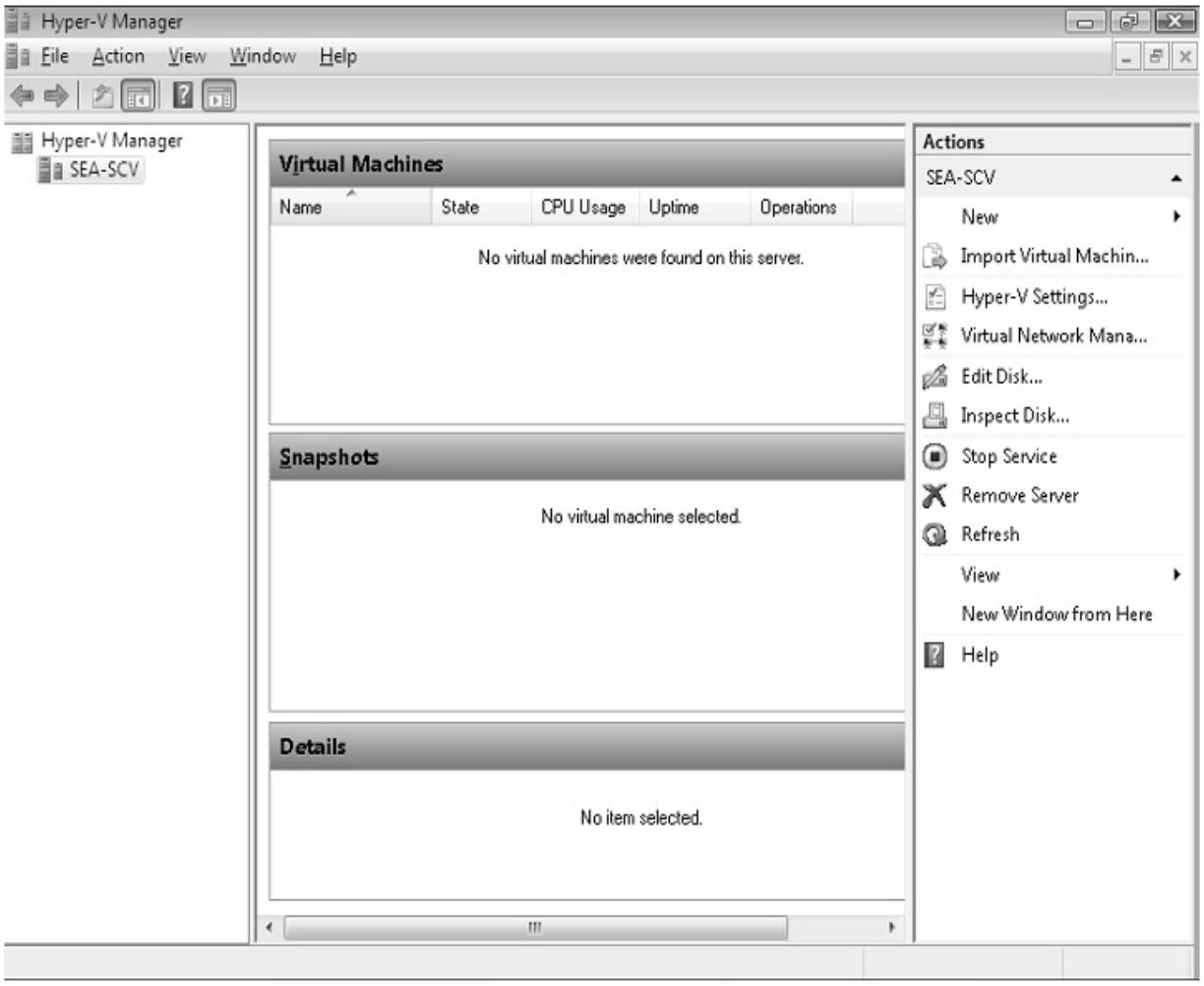


Рисунок 20 - Управляющая консоль Hyper-V

Для создания новой виртуальной машины следует выбрать New | Virtual Machine. Процесс создания виртуальной машины проходит согласно следующим этапам:

- Название виртуальной машины.
- Определение местоположения конфигурационных файлов виртуальной машины.
- Выделение памяти.
- Настройка сети.
- Настройка системы хранения данных.
- Установка операционной системы.

В ходе создания виртуальной машины требуется указать

месторасположение для двух типов файлов: конфигурационные файлы виртуальной машины и файл виртуального жесткого диска.

Это можно сделать либо при создании виртуальной машины, либо задать по умолчанию для всех создаваемых виртуальных машин как показано на рисунке 21.

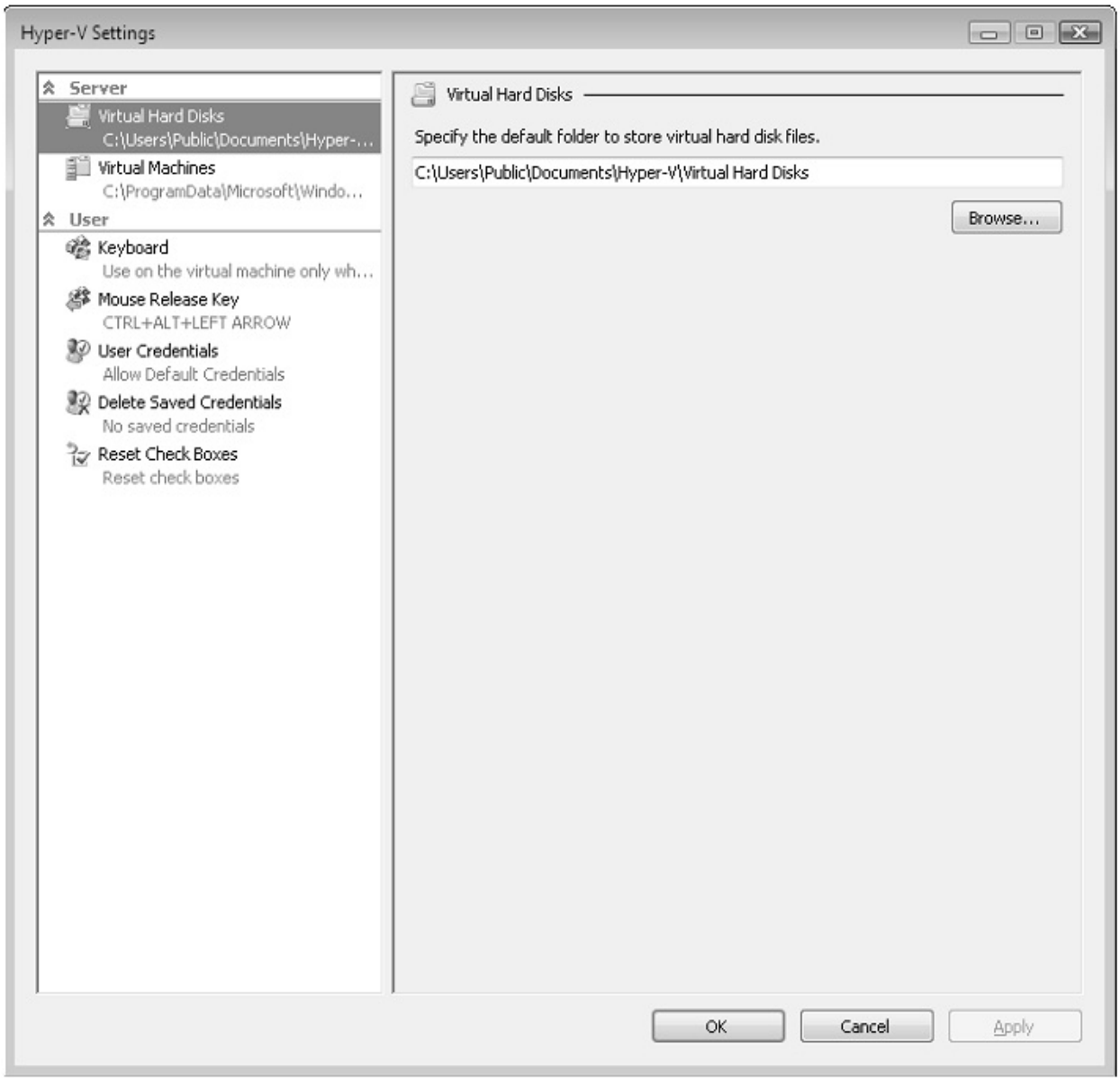


Рисунок 21 - Настройка расположения конфигурационных файлов ВМ

Для доступа к виртуальным машинам необходимо настроить на них доступ из сети. В Hyper-V существует три вида сети:

- Внешняя виртуальная сеть (External virtual networks).
- Внутренняя виртуальная сеть (Internal virtual networks).
- Частная виртуальная сеть (Private virtual networks).

Внешняя виртуальная сеть - виртуальная сеть, имеющая выход «во внешний мир». При создании сети типа External необходимо указать сетевой интерфейс, через который будет осуществляться выход наружу. При этом

физический интерфейс теряет все сетевые настройки, и создается виртуальный адаптер в хостовой ОС, к которому привязываются все необходимые протоколы и настройки. Физический же интерфейс остается всего с одним протоколом: Virtual Network Switching Protocol [2].

Кроме этого, в Windows Server 2008 R2 появилась возможность создавать сети типа External, но при этом все равно изолировать их от хостовой ОС. Делается это снятием галочки «Allow management operating system to share this network adapter.

Внутренняя виртуальная сеть - сеть, к которой могут подключаться только виртуальные интерфейсы – виртуальных машин и хостовой ОС. К физическому интерфейсу сеть типа Internal не привязывается, и, соответственно, выхода «вовне» не имеет.

Частная виртуальная сеть - то же самое, что и Internal, за исключением того, что к такой сети могут подключаться только виртуальные машины. Сеть типа Private не имеет доступа ни к «внешнему миру», ни к хостовой ОС. В таблице 2 приведена сравнительная характеристика все видов виртуальных сетей.

Таблица 2 - Типы виртуальных сетей

Тип виртуальной сети	Между ВМ на хост машине	Между ВМ и родительским разделом	Между ВМ и внешней сетью
External	✔	✔	✔
Internal	✔	✔	
Private	✔		

3.6 (продолжаем 3й пункт) ЛОКАЛЬНАЯ ВИРТУАЛИЗАЦИЯ НАСТОЛЬНЫХ СИСТЕМ ПРИМЕНИТЕЛЬНО К КАФЕДРЕ

6.1 Преимущества и использование

Применительно к кафедре, локальная виртуализация настольных систем принесет наибольшую выгоду используя технологию App-V. Виртуализация приложений позволит упростить развертывание, администрирование, обновление и удаление приложений, используемых на кафедре во время работы и обучения.

Локальная виртуализация приложений позволяет:

- Централизованно управлять установкой программных продуктов на всей кафедре.
- Поддерживать все программные продукты в актуальном состоянии и устранить проблемы, возникающие при разных установленных версиях одной и той же программы.
- Централизованно управлять удалением программных продуктов.
- Централизованно распределять права доступа тех или иных пользователей к тем или иным программным продуктам.
- Поддерживать клиентские компьютеры в чистом состоянии, так как необходимость установки программных продуктов непосредственно на них отпадает.

Рассмотрим приложения, наиболее подходящие на роль виртуализированных приложений.

Таблица 3 - Список приложений

Название приложения
1 MS Visual Studio 2010
2 MS Office 2010
3 Foxit Reader
4 Toad
5 MS SQL Management Studio

Рассмотрим сценарии использования вышеописанных виртуализированных приложений.

Виртуализация приложений может предоставить качественно новый способ использования программных продуктов. Чтобы убедиться в этом сначала посмотрим на традиционную модель.

В традиционной модели на каждый клиентский компьютер необходимо установить отдельную копию приложения. Соответственно каждый программный продукт занимает на компьютере определённое количество места, требует персонального администрирования, обновления и так далее. Все это занимает время и при возникновении неисправностей требует длительного времени их устранения как показано на рисунке 3.1.

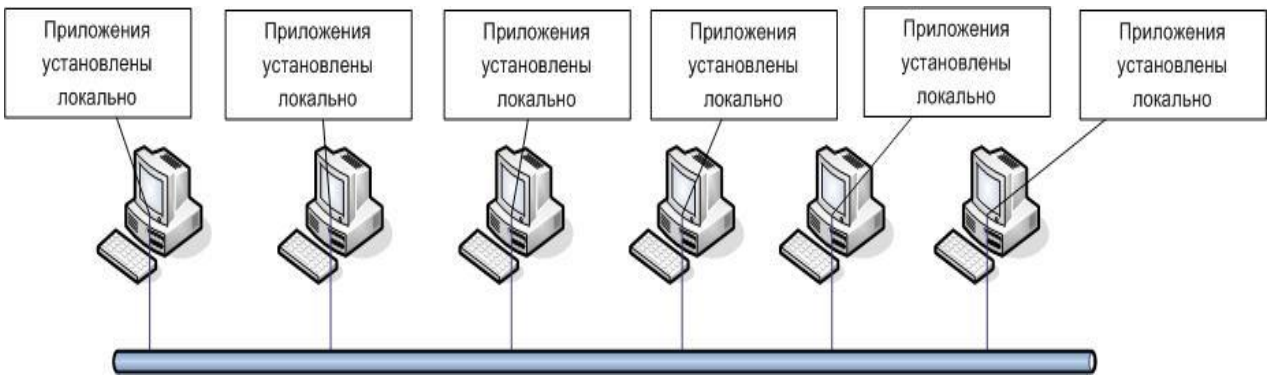


Рисунок 22 - Традиционная модель

Как видно из рисунка, при традиционной модели развертывания приложений время, требуемое на процедуру, растет пропорционально количеству машин в организации. Любые операции по обслуживанию будут занимать огромное количество времени и сил.

Виртуализация приложений позволяет централизовать данный процесс и значительно сократить время, требуемое на развертывание и обслуживание.

Развертывание приложений с помощью App-V.

В отличие от традиционной модели развертывания, виртуализация предлагает совершенно иной подход. Все приложения, требующиеся пользователям, централизованно устанавливаются на сервер приложений один единственный раз. В данном случае кафедральный администратор заранее готовит и устанавливает приложения на сервер, после чего публикует их на клиентские машины. При необходимости в приложении, например, началась пара по программированию, клиентские компьютеры запрашивают данное приложение с сервера, сервер в потоковом режиме передает необходимые для запуска данные и компьютер клиента выполняет приложение использую свои вычислительные мощности, рисунок 23.

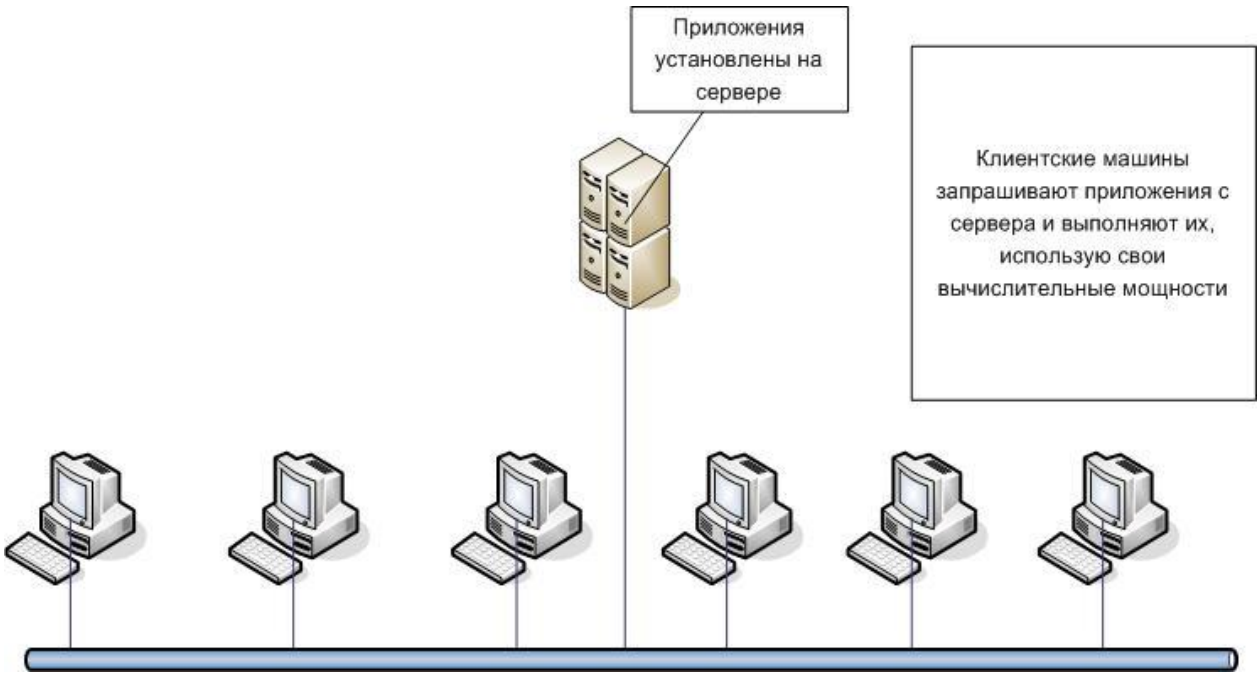


Рисунок 23 - Локальная виртуализация приложений

Так как приложения выполняются, используя ресурсы клиентских машин, нагрузка на сервер снижается. Принимая во внимание тот факт, что некоторые вышеуказанные приложения могут иметь значительные требования к ресурсам, такой подход позволяет разгрузить центральный сервер для выполнения других задач. С учетом того, что север приложений является виртуальным сервером, наряду с серверами баз данных, это значительно снижает нагрузку с физических серверов.

6.2 Работа с App-V

Для работы с виртуальными приложениями используется специальная консоль управления. Она позволяет выполнять основные функции для развертывания программ:

- Импорт приложения - процесс преобразования приложения, чтобы оно могло быть доступно для потоковой передачи с сервера. Необходимы файлы .osd или .sprj. При импорте нового приложения создаются автоматически.
- Ручное добавление приложения - процесс ручного импорта приложений. Необходимо явно указать всю требуемую информацию для импорта.
- Предоставление и запрет доступа к приложению - ограничение доступа к приложению конкретным пользователям или группам, что показано на рисунке 24.

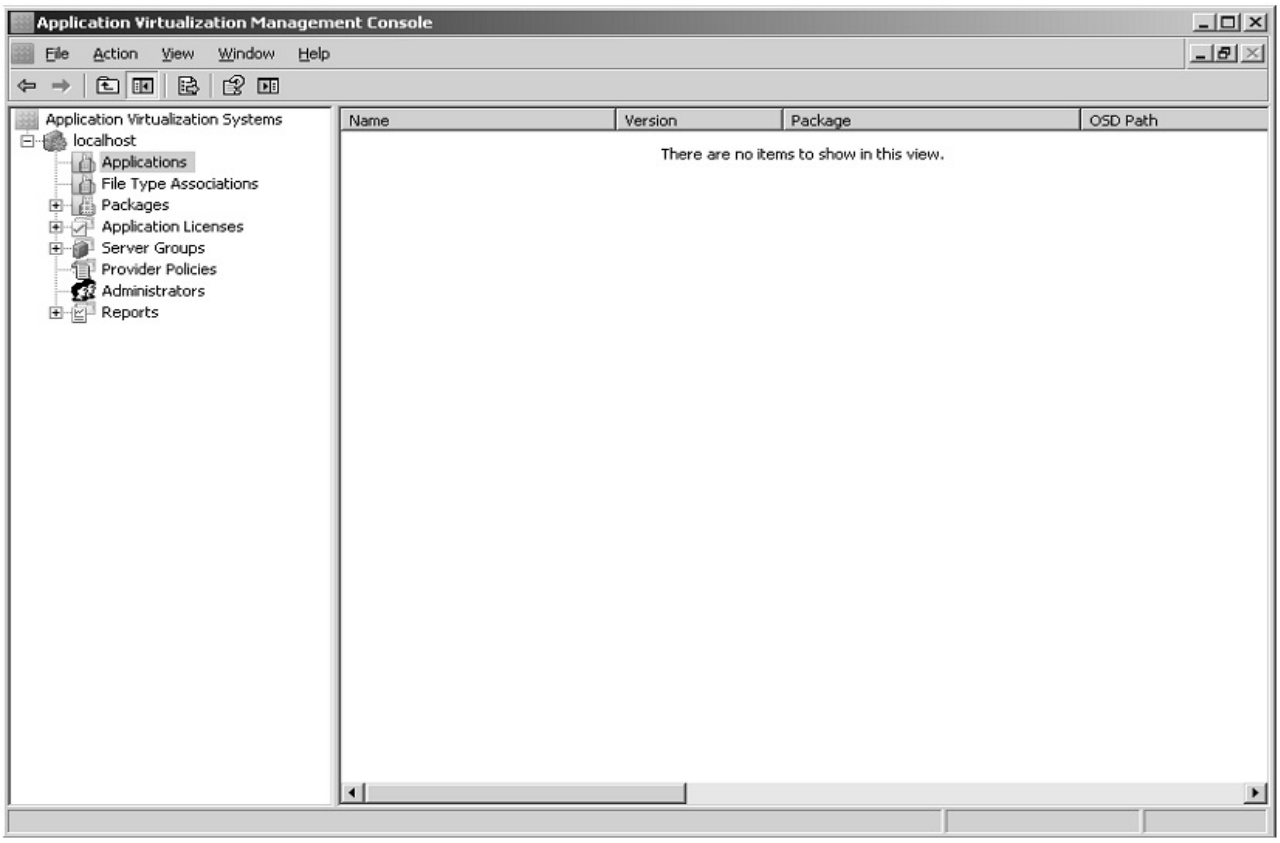


Рисунок 24 - Консоль управления виртуализацией приложений

Для успешного импорта приложения необходимо указать его .osd или .sprj файл. Использую .osd файл администратор вынужден будет добавлять каждое приложение в пакете отдельно, использую .sprj файл возможно установить весь пакет целиком, как показано на рисунке 25.

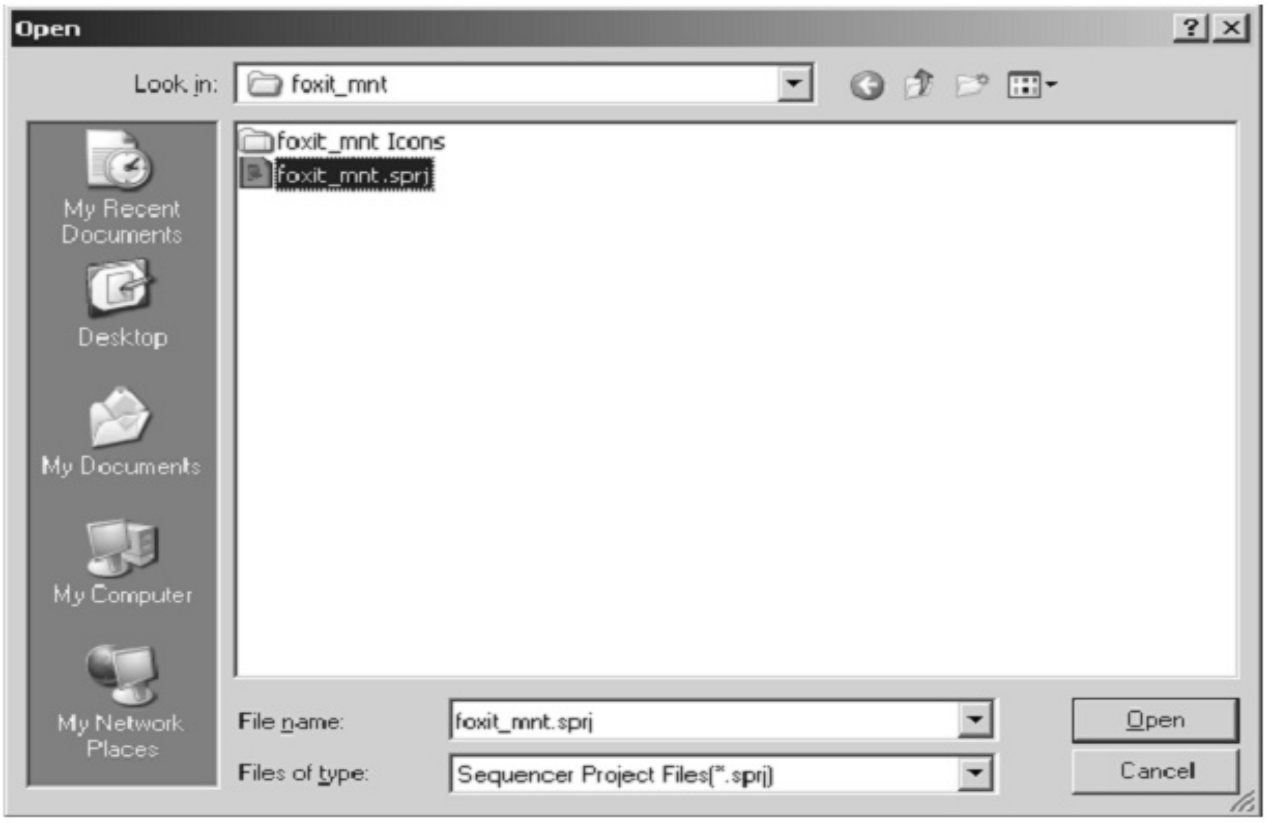


Рисунок 25 - Выбор нужного файла

В ходе импорта приложения необходимо указать дополнительную информацию, а также желательно дать описание приложению, как показано на рисунке 26.

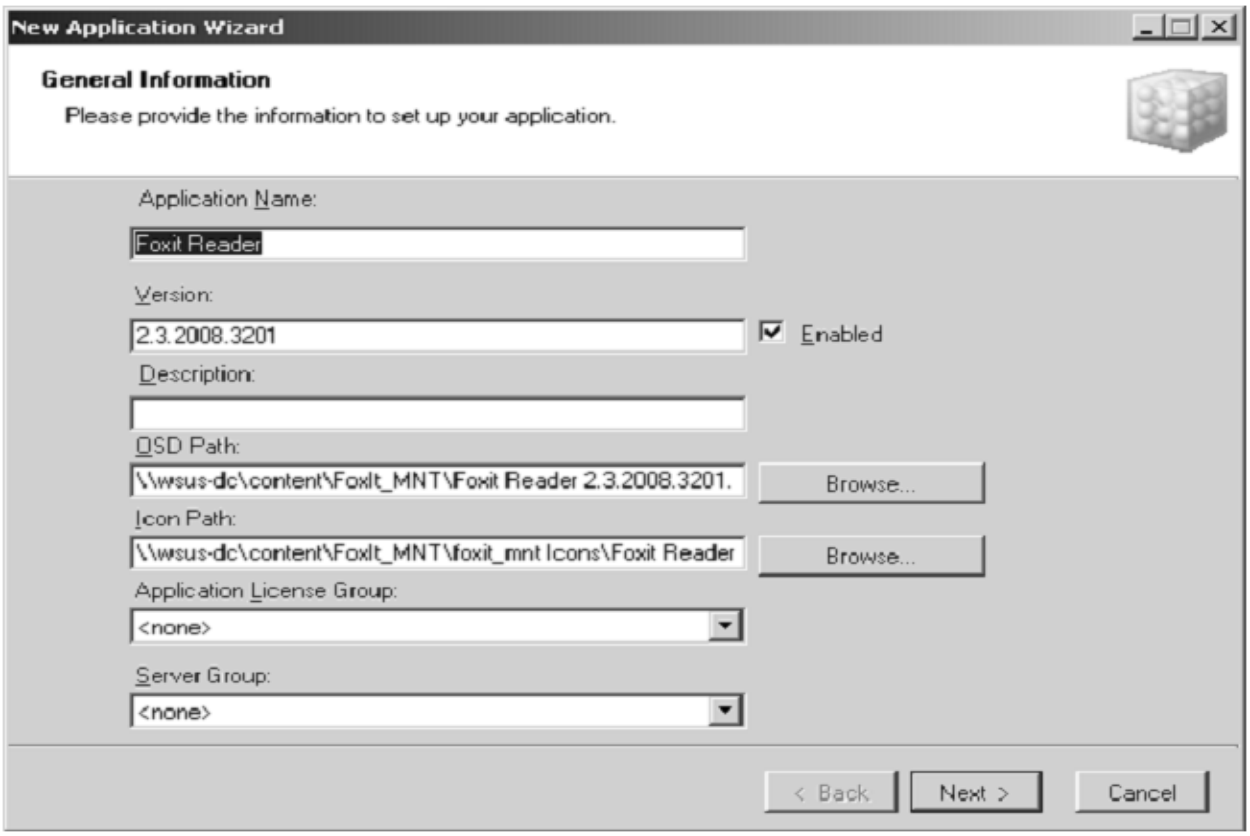


Рисунок 26 - Описание приложения и прочие параметры

В процессе импорта администратор имеет возможность указать местоположения ярлыков приложения и других файлов на клиентских машинах, как показано на рисунке 27.

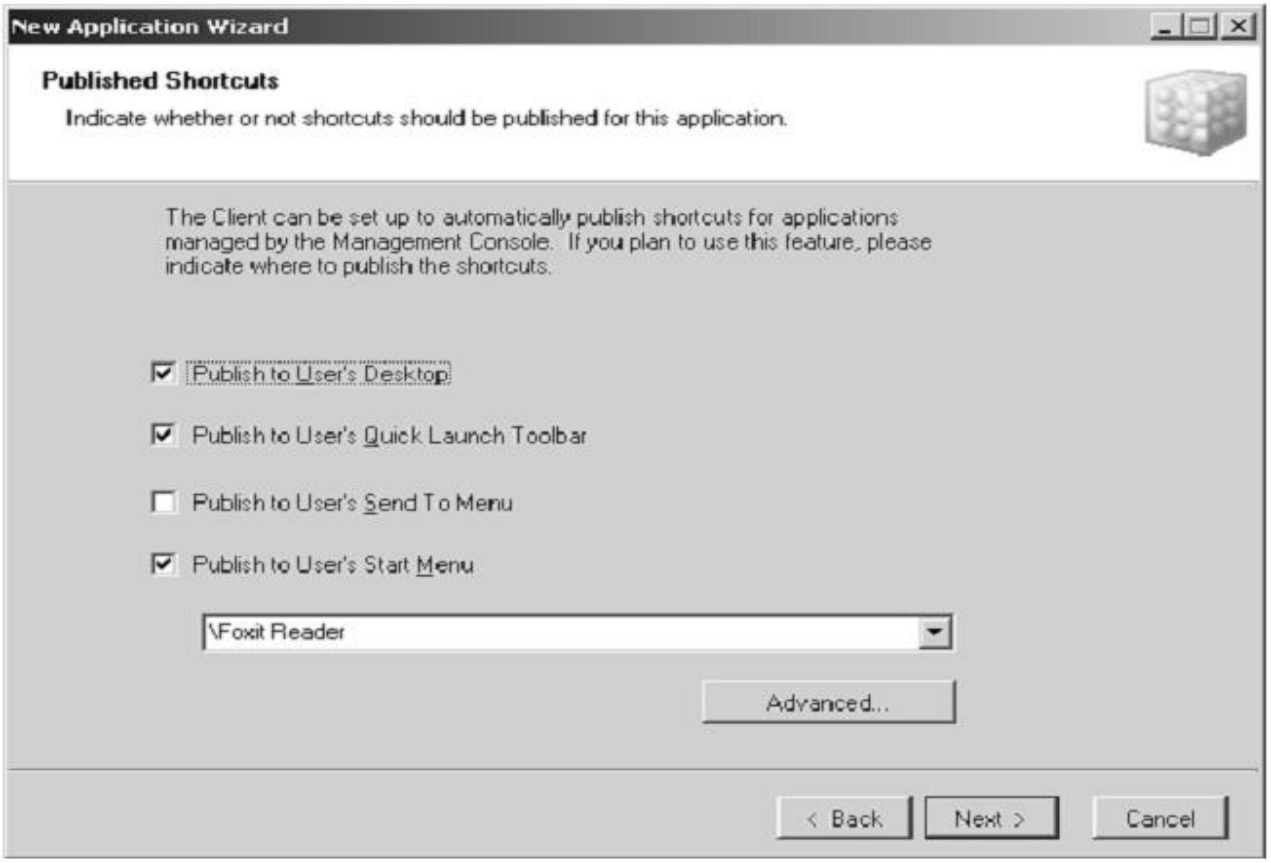


Рисунок 27 - Настройки приложения на клиентских компьютерах

Для устранения конфликтов относительно разрешений файлов, настоятельно рекомендуется указать в ходе импорта настройки ассоциации. Это устранит возможные конфликты в будущем и позволяет поддерживать рабочую среду целостной на всех машинах. Подобные меры значительно упрощают администрирование, делая его более прозрачным. Мастер по установке виртуального приложения позволяет сделать это сразу во время установки. Наилучшей практикой считается сделать это именно на этом этапе. На рисунке 28 показано окно настроек ассоциаций файлов.

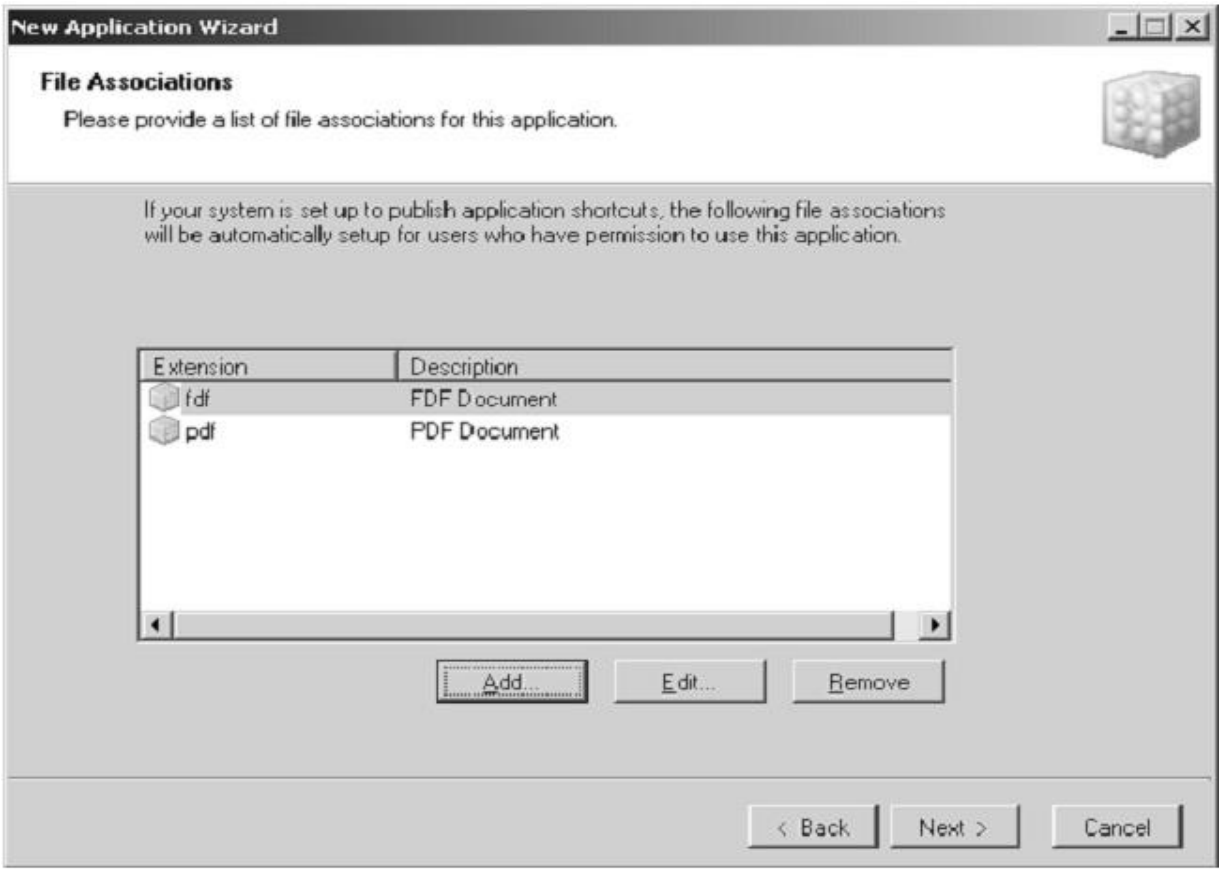


Рисунок 28 - Настройка ассоциаций файлов

Для ограничения доступа к приложениям используются группы и пользователи из настроек контроллера домена сети. Интеграция с Active Directory позволяет гибко настраивать доступ к приложениям. К примеру возможно запретить доступ студентов младших курсов к приложениям по работе с базами данных, в то время как офисные приложения будут доступны всем пользователям. Пример настроек показан на рисунке 29.

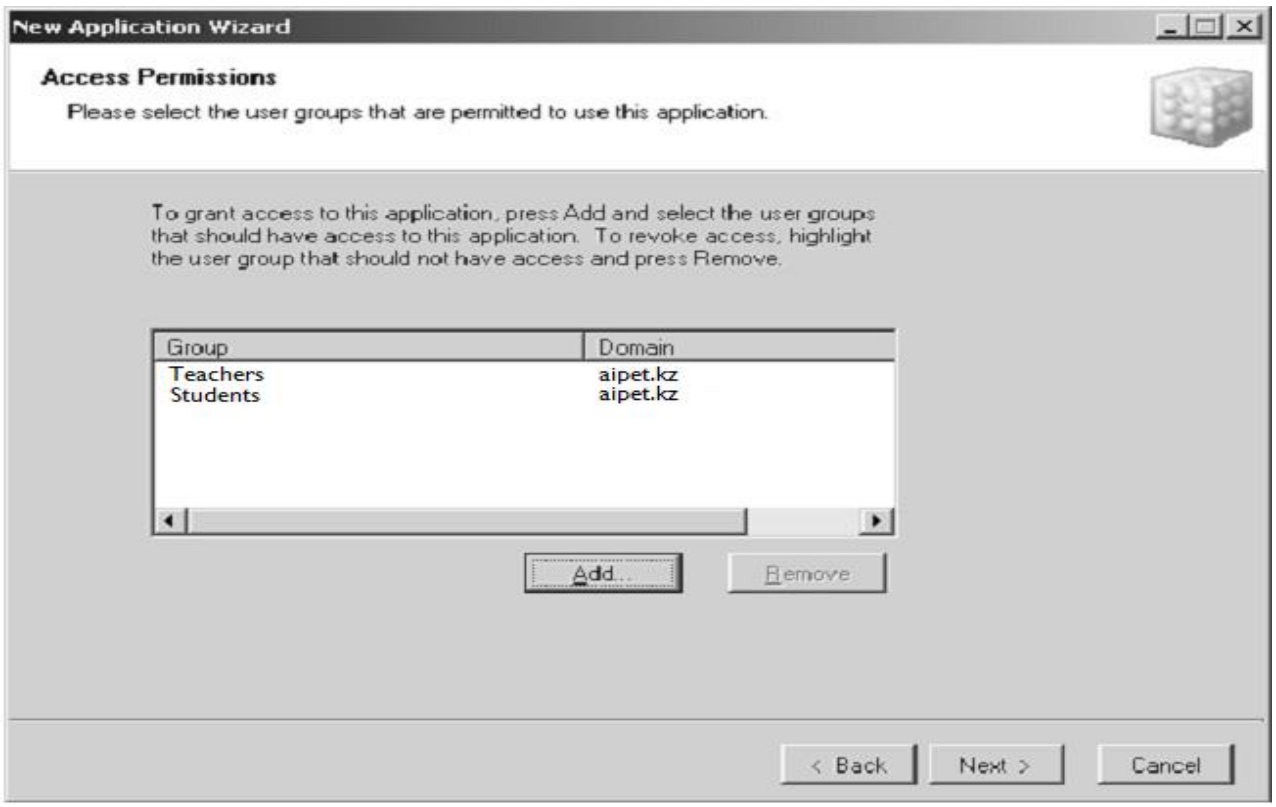


Рисунок 29 - Настройки доступа к приложению

После предоставления всех необходимых сведений рекомендуется еще раз проверить все настройки. При возникновении конфликтов система выдаст соответствующее предупреждение, как показано на рисунке 30.

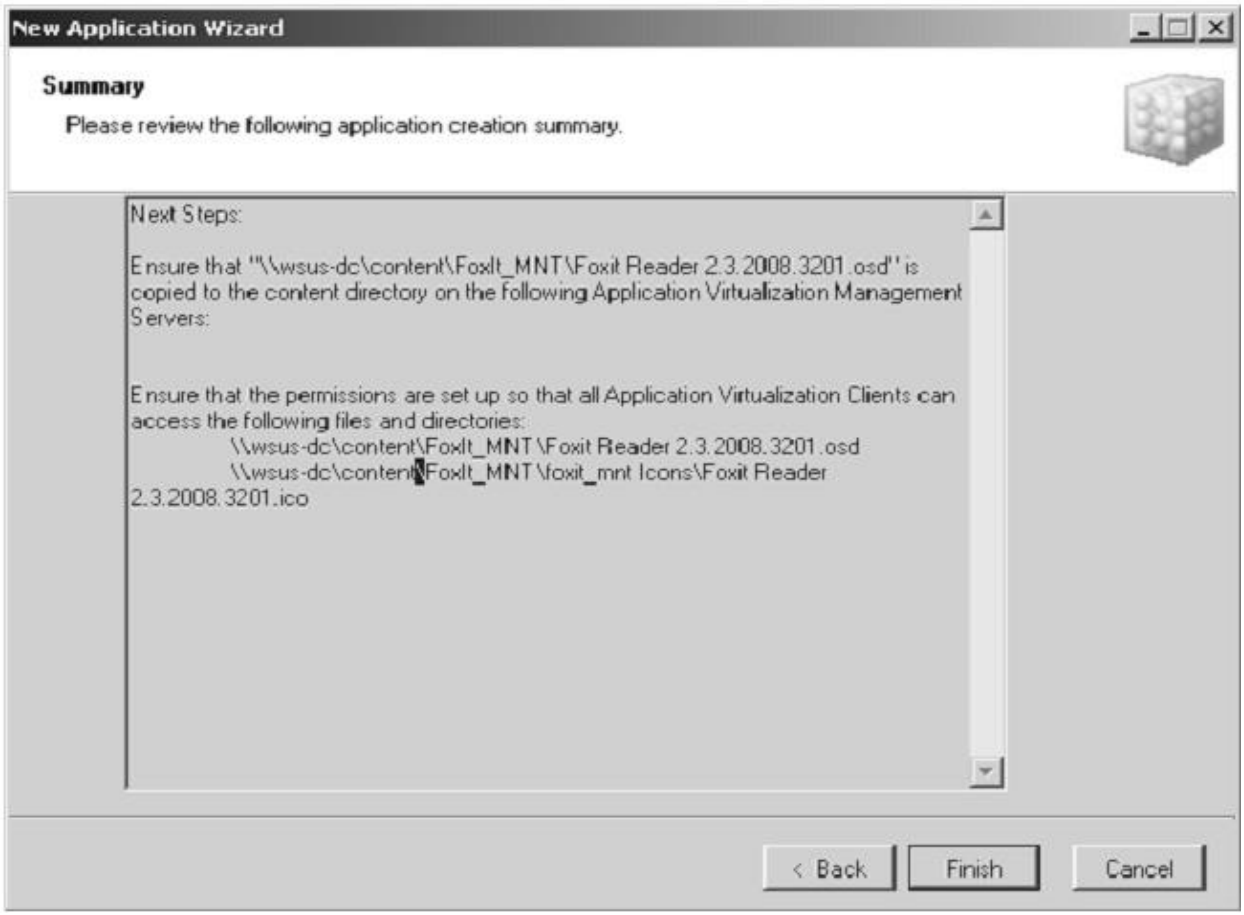


Рисунок 30 - Сводная информация по приложению

Приложение готово к передаче клиентам, как видно из рисунка 31.

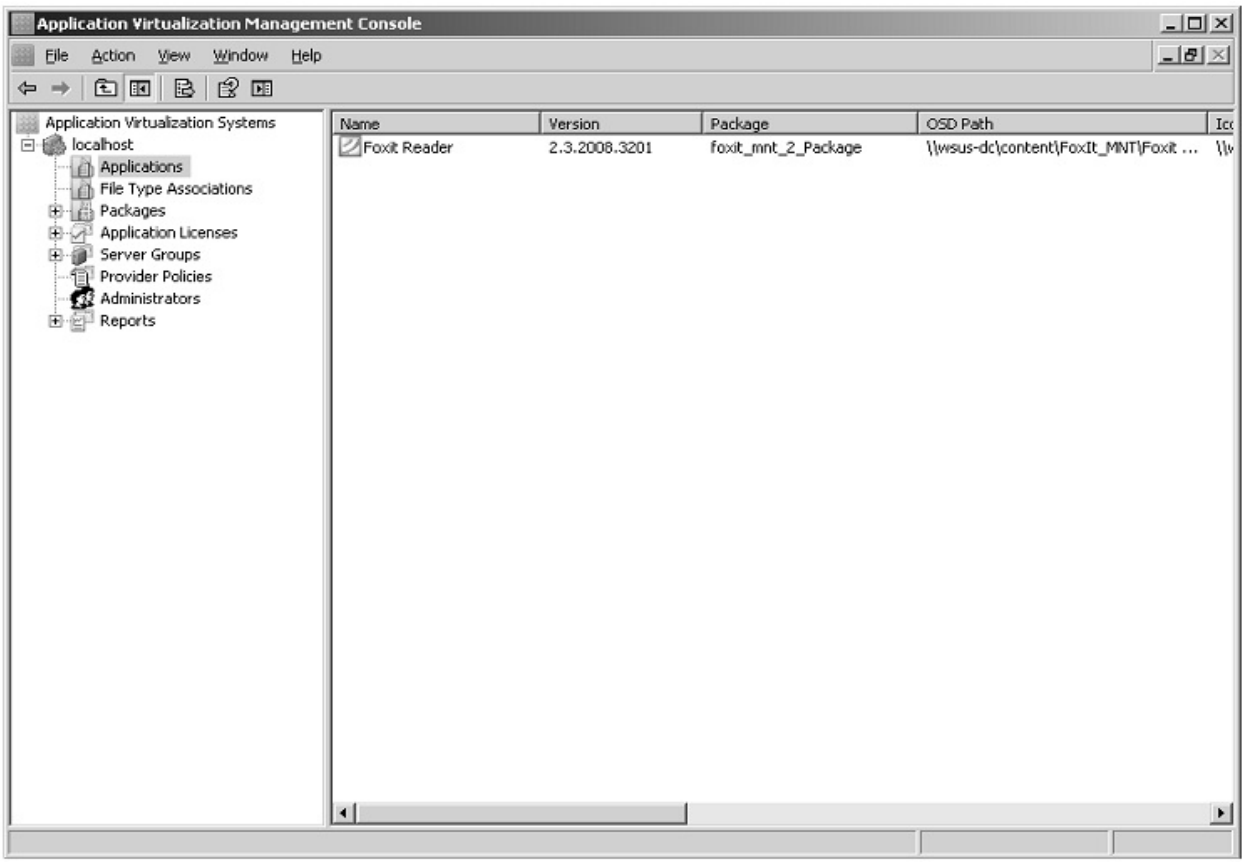


Рисунок 31 - Приложение готово к передаче клиентам

Чтобы клиенты имели возможность запросить приложение с сервера необходимо установить клиентскую программу. Она входит в MDOP (Microsoft Desktop Optimization Pack). Данный пакет распространяется бесплатно при условии, что у клиента есть активная корпоративная лицензия.

Стоит отметить, что в данном варианте реализации для выполнения приложений используются ресурсы локальных компьютеров. Данное решение оправдано, если сервер не располагает дополнительными вычислительными мощностями. Сервер только потоково рассылает приложения клиентам.

Возможен другой способ реализации, при котором нагрузка на выполнение приложений ложится на сам сервер. Данный вид реализации потребует еще одного сервера и, разумеется, значительно более мощный сервер приложений.

В случае кафедры первый вариант более целесообразен, так как позволяет с пользой использовать имеющиеся локальные машины, в то же время, экономя на приобретении дополнительных вычислительных мощностей для центральных серверов.

Так как безопасность является основным требованием при работе с серверами баз данных, а непрерывность работы и минимизация времени простоя является основным требованием в учебных заведениях необходимо принять определенные меры по обеспечению отказоустойчивости системы. Для решения этой проблемы было решено использовать кластеризацию.

Кластеризация, по сути, представляет собой способ объединения

нескольких отдельных машин в единую, отказоустойчивую систему. Каждая машина в кластере представляет собой узел, при выходе которого из строя, нагрузку и сервисы это узла берут на себя другие узлы кластера, обеспечивая, таким образом, беспрерывную работу системы.

Для создания кластера на основе серверов виртуализации Hyper-V необходимо следующее:

- Минимум два сервера с установленной операционной системой Microsoft Windows Server 2008 R2 Enterprise или Datacenter Edition с установленной ролью Hyper-V и компонентом Failover Clustering. Следует использовать одинаковую версию операционной системы на всех узлах — нельзя на один узел ставить Enterprise Edition, а на другой Datacenter. Узлы должны быть одинаковой архитектуры — нельзя использовать в качестве одного узла Itanium сервер, а в качестве другого — x64. Кроме того, одинаковый способ установки должен быть использован на всех узлах — нельзя на один узел ставить Server Core, а на другой Full Installation. Аппаратное обеспечение узлов также должно быть как можно более идентичным. Все узлы кластера должны входить в один домен системы AD DS.
- Внешнее хранилище данных, состоящее как минимум из двух логических юнитов. Хранилище должно включать в себя один логический юнит, настроенный как диск-свидетель. Данный диск содержит копию диска с конфигурацией кластера. Помимо этого должен быть еще один логический юнит, хранящий виртуальные машины и их виртуальные жесткие диски.

Сетевая инфраструктура, соединяющая все компоненты кластера должна быть, включая внешнее хранилище данных, может быть реализована несколькими способами. Тем не менее она должны быть спроектирована таким образом, чтобы обеспечить отказоустойчивость, и желательно, избыточность линий.

Для кафедры предлагается использовать простой кластер, состоящий из двух узлов. Это обеспечит требуемый уровень отказоустойчивости при минимально возможных затратах. Показано на рисунке 32.

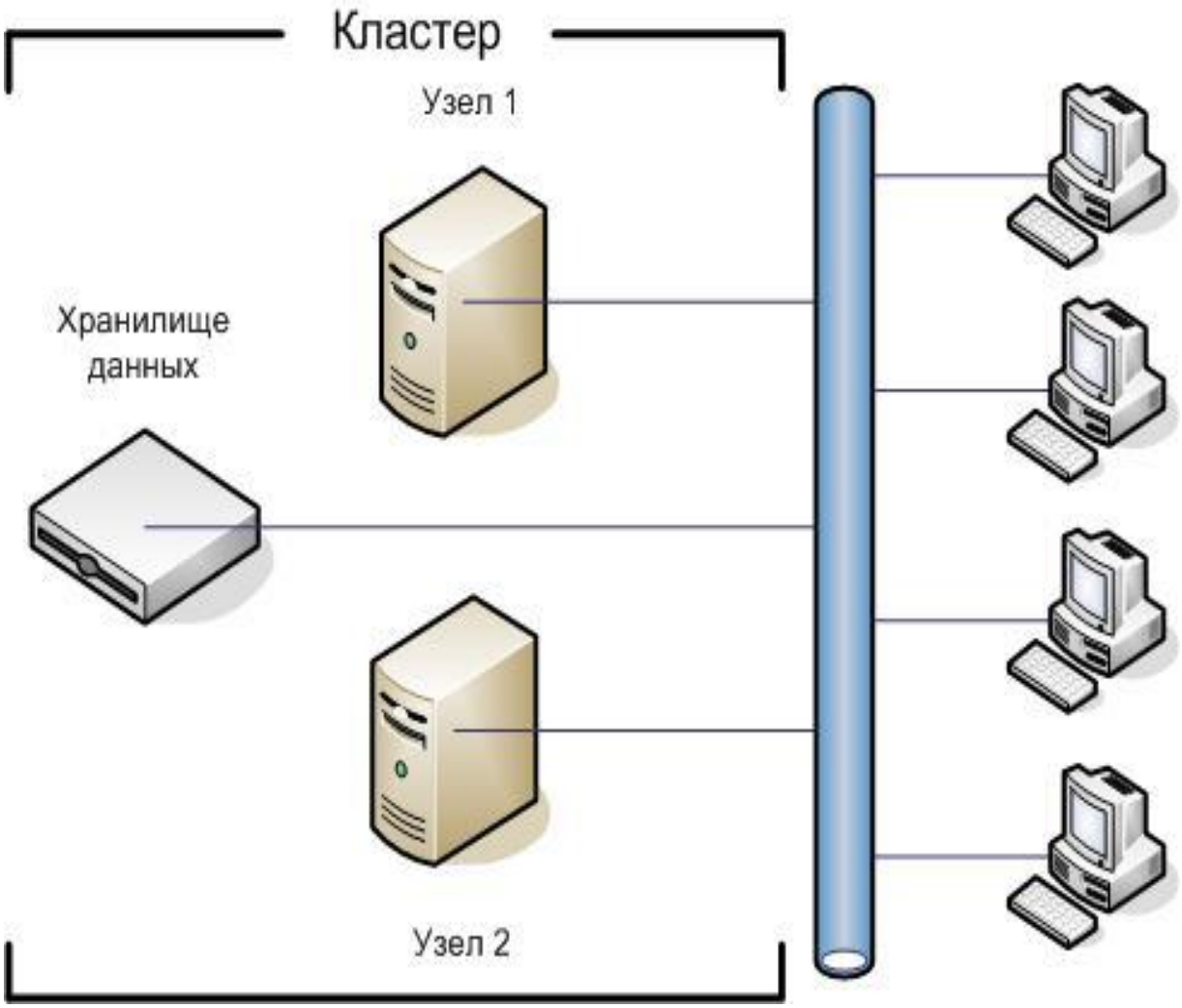


Рисунок 32 - Схематическое изображение кластера

Используя кластер возможно переносить работающие виртуальные машины между узлами не прерывая работы пользователя. Для этого необходимом настроить виртуальную машину с использованием Live Migration. Для снижения времени простоя при администрировании серверов, кафедральные сервера баз данных рекомендуется располагать в виртуальных машинах, настроенных на использование с Live Migration.

Для этого необходимо:

1 Настроить кластер с учетом требований, описанных выше.

2 Установить Windows Server 2008 R2 с ролью Hyper-V на каждую машину.

3 Установить компонент Failover Clustering на каждую машину и настроить сервера как узлы в кластере. Рекомендуется проверить правильность настройки используя встроенный мастер Validate A Configuration Wizard, как показано на рисунке 33.

4 Используя контрольную панель, активировать Cluster Shared Volumes. Это даст возможность всем узлам в кластере использовать общее внешнее хранилище. Сделать это можно только один раз на каждом кластере.

5 Добавить хранилище из списка возможных хранилищ использую соответствующие элементы контрольной панели.

6 Создать виртуальные машины, которые должны использовать функции Live Migration. Для хранения файлов конфигурации и виртуальных жестких дисков необходимо выбрать общее хранилище, которое было настроено выше. Виртуальная машина должна быть создана на узле, имеющем доступ к общему хранилищу.

7 Необходимо настроить виртуальную машину как высоко доступную, использую контрольную панель и вкладки Configure A Service Or Application. Это необходимо сделать со всеми виртуальными машинами, которые планируется использовать с Live Migration.

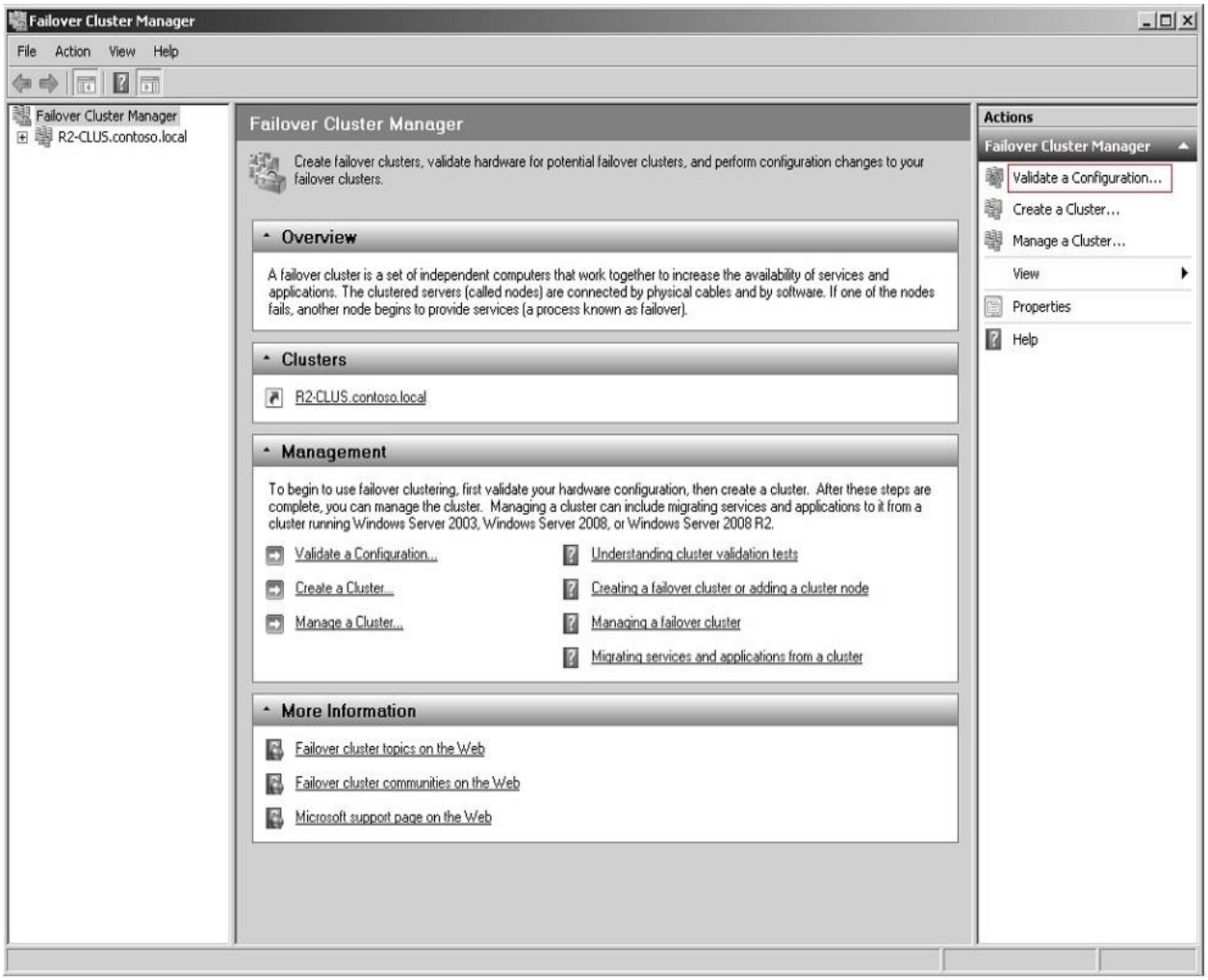


Рисунок 33 - Использование мастера Validate A Configuration Wizard

8 Необходимо указать для какой виртуальной машины какая кластерная сеть должна использоваться, как показано на рисунке 34.

На этом этапе настройку кластера и виртуальных машин, работающих с функцией Live Migration можно завершить. В результате все виртуальные машины, настроенные вышеописанным способом, имеют повышенную отказоустойчивость и при правильном администрировании могут работать практически беспрерывно.

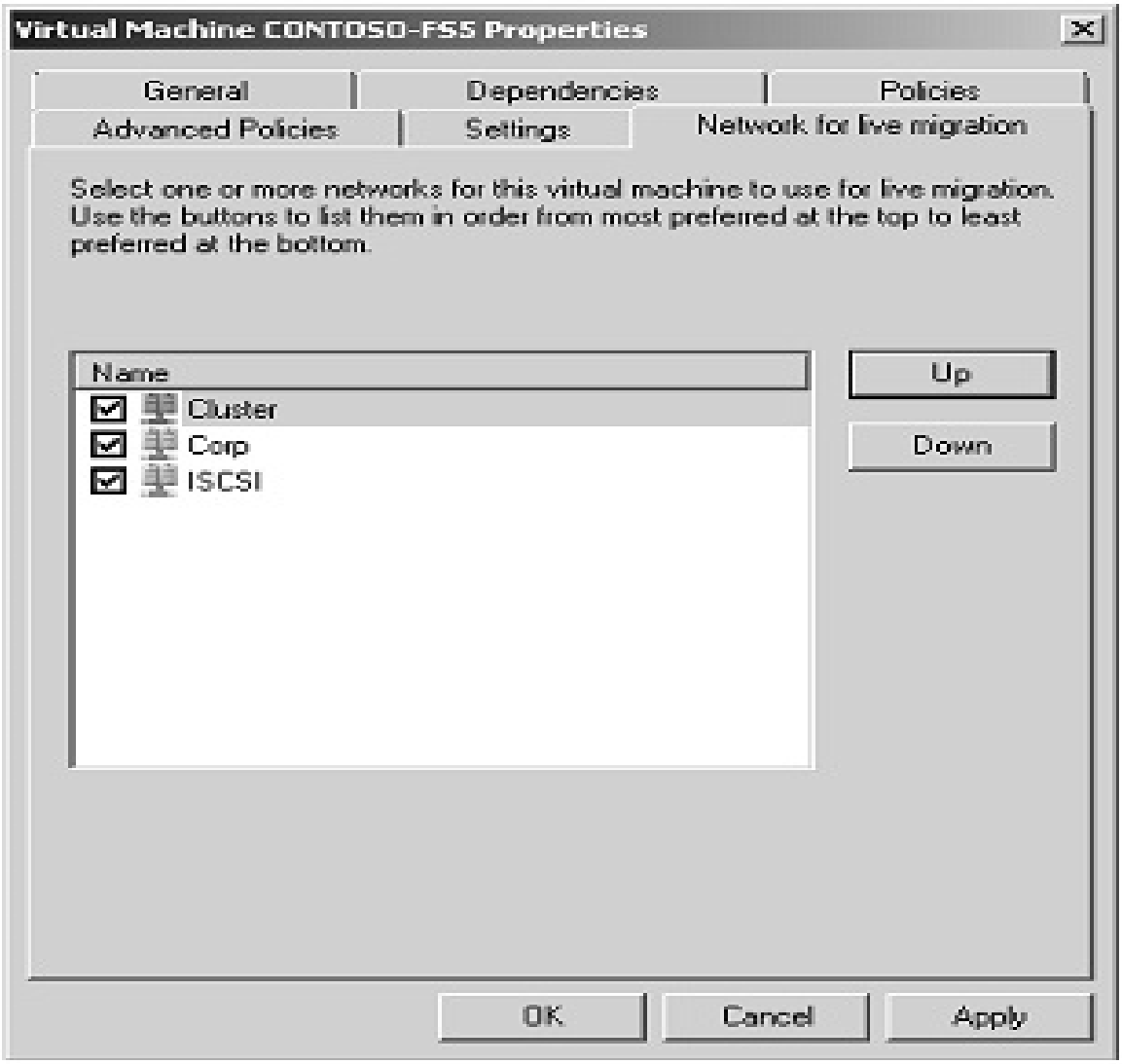


Рисунок 34 - Выбор кластерной сети

Чтобы перенести виртуальные машины с одного узла кластера на другой не прерывая работы необходимо сделать следующее:

1 Открыть панель управления кластером

2 Выбрать нужную виртуальную машину и выполнить Live Migrate Virtual Machine To Another Node. Затем указать узел куда необходимо перенести машину, как показано на рисунке 35.

3 Процесс перемещения виртуальной машины будет показан в центральной части панели управления, как показано на рисунке 36.

Время, необходимое для переноса виртуальной машины, зависит от количества оперативной памяти, настроенной для виртуальной машины, нагрузки на обоих узлах, а так же пропускной способности сетевого канала, соединяющего узлы кластера.

4 После завершения переноса, владельцем виртуальной машины становится второй узел, как показано на рисунке 37.

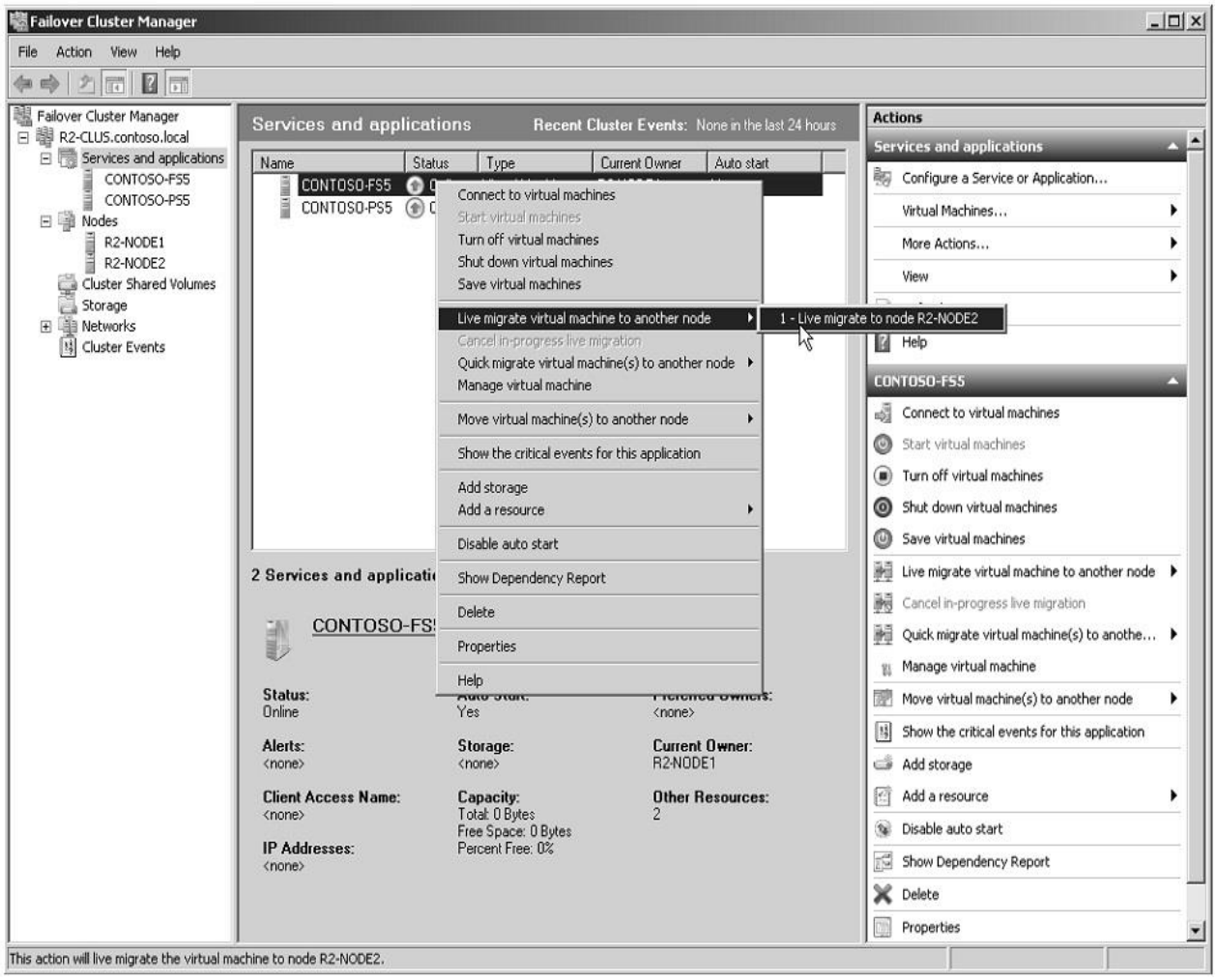


Рисунок 35 - Live Migration в действии

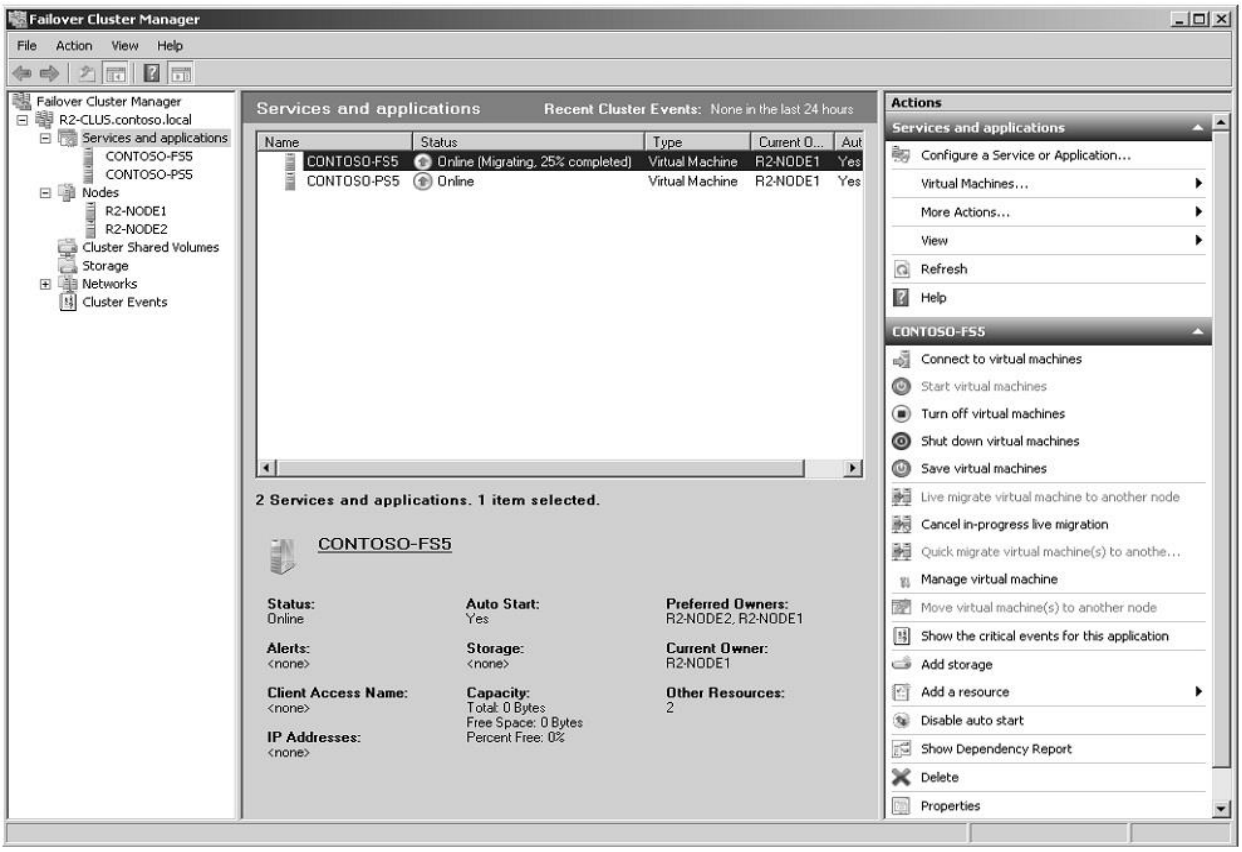


Рисунок 36 - Процесс переноса виртуальной машины

В версии R2 появилась возможность переносить виртуальные машины с использованием Windows PowerShell. Это можно выполнить следующей командой:

Get-Cluster "<Cluster Name>" | Move-ClusterVirtualMachineRole -Name "<VM group name>" -Node "<Destination node name>"

В вышеуказанной команде <Cluster Name> имя узла, на котором находится виртуальная машина. <VM group name> название группы виртуальной машины и <Destination node name> имя узла в кластере, куда необходимо переместить виртуальную машину, используя Live Migration.

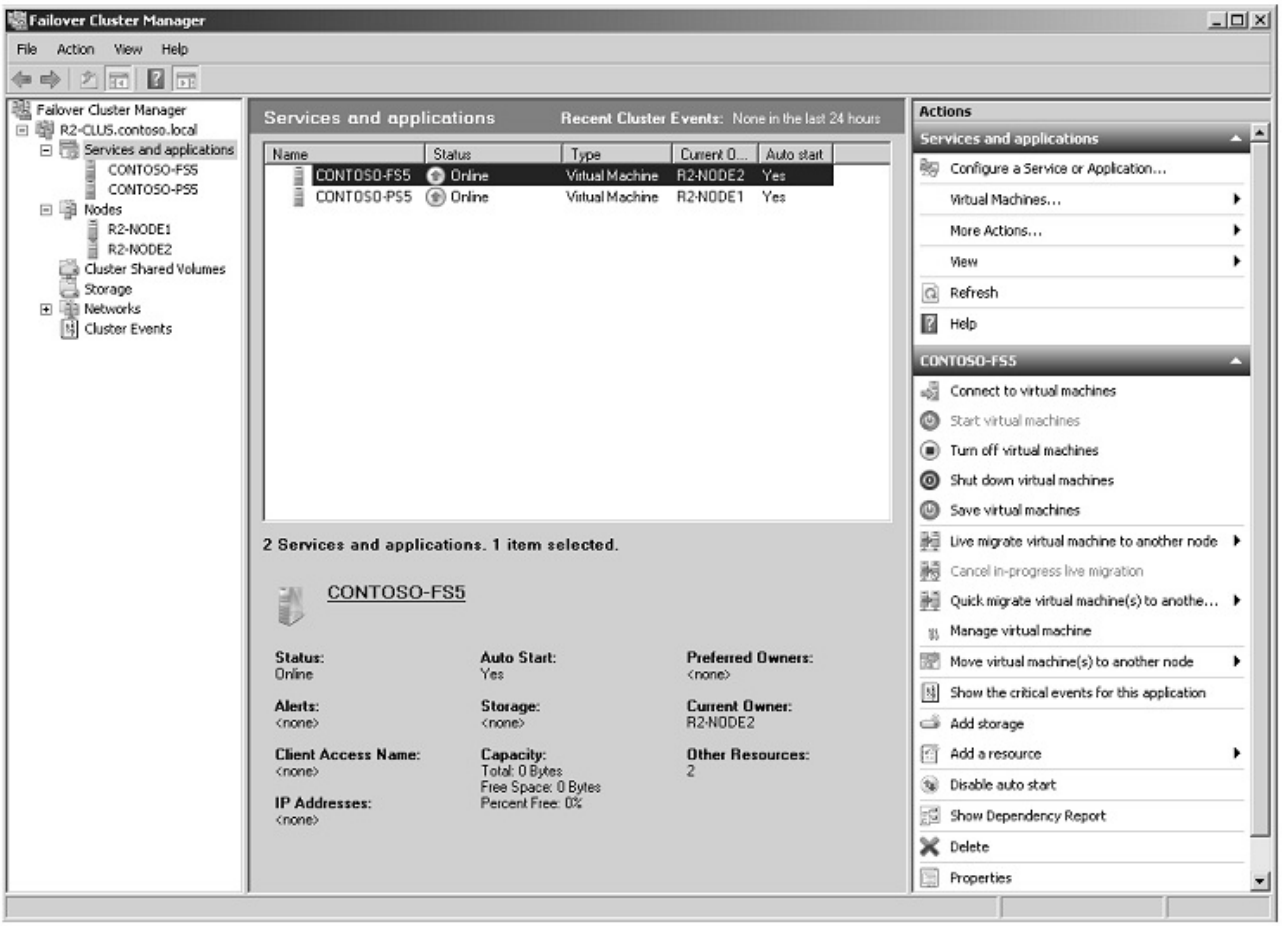


Рисунок 37 - Результат переноса виртуальной машины

4.3 Контроль доступа, раздача прав при работе через vCenter

VCenter предлагает достаточно гибкую систему раздачи прав. Что она собой представляет, показано на рисунке 38. Здесь виден список привилегий (прав), включенных в роль Administrator.

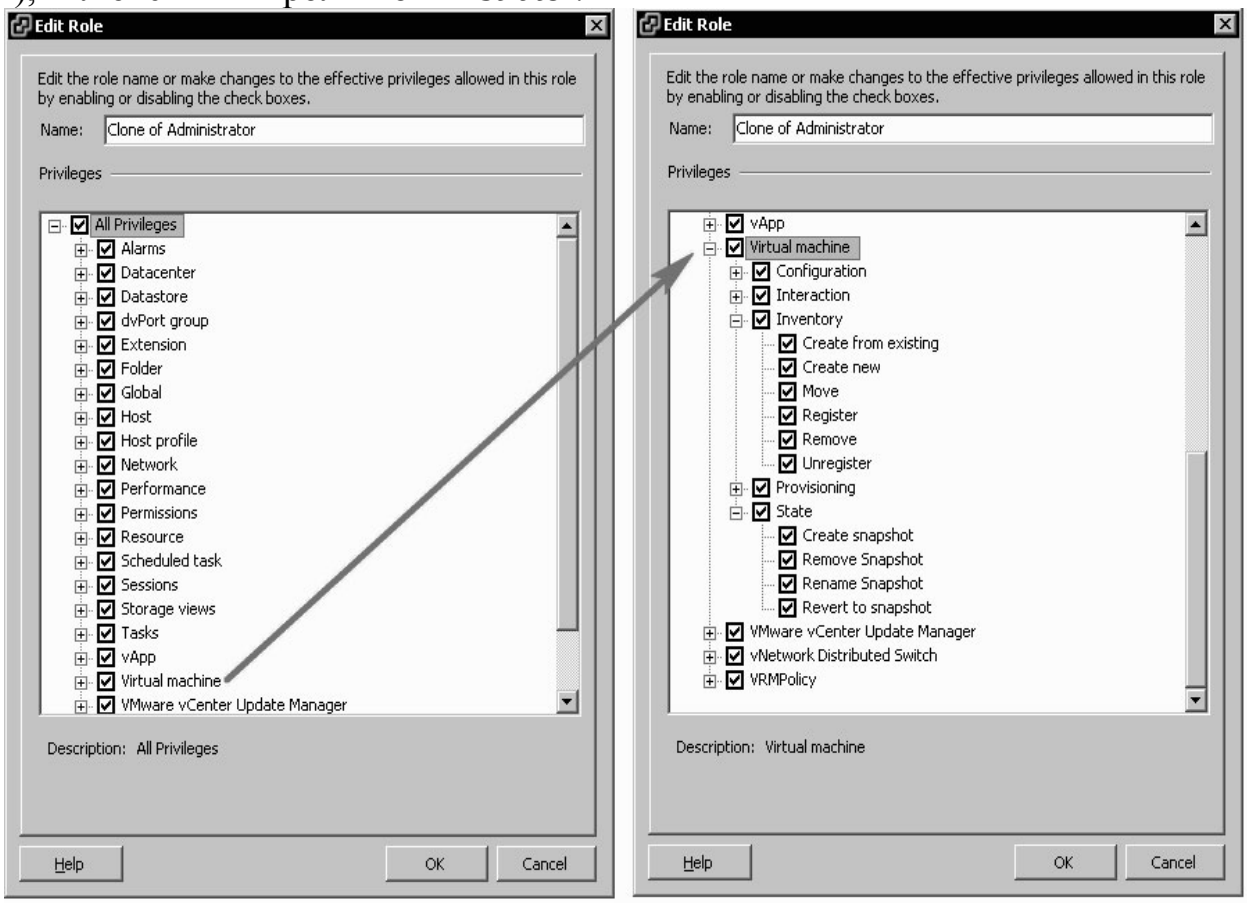


Рисунок 38. Настройки привилегий на vCenter

Привилегия – это право на атомарное действие. На рисунке справа показаны привилегии для виртуальных машин, такие как «Создать», «Удалить», «Создать снимок состояния (snapshot)» и др. Набор каких-то привилегий называется ролью.

Роль – это конкретный набор привилегий, то есть разрешенных действий.

Роль можно дать пользователю или группе на какой-то уровень иерархии vCenter как показано на рисунке 39.

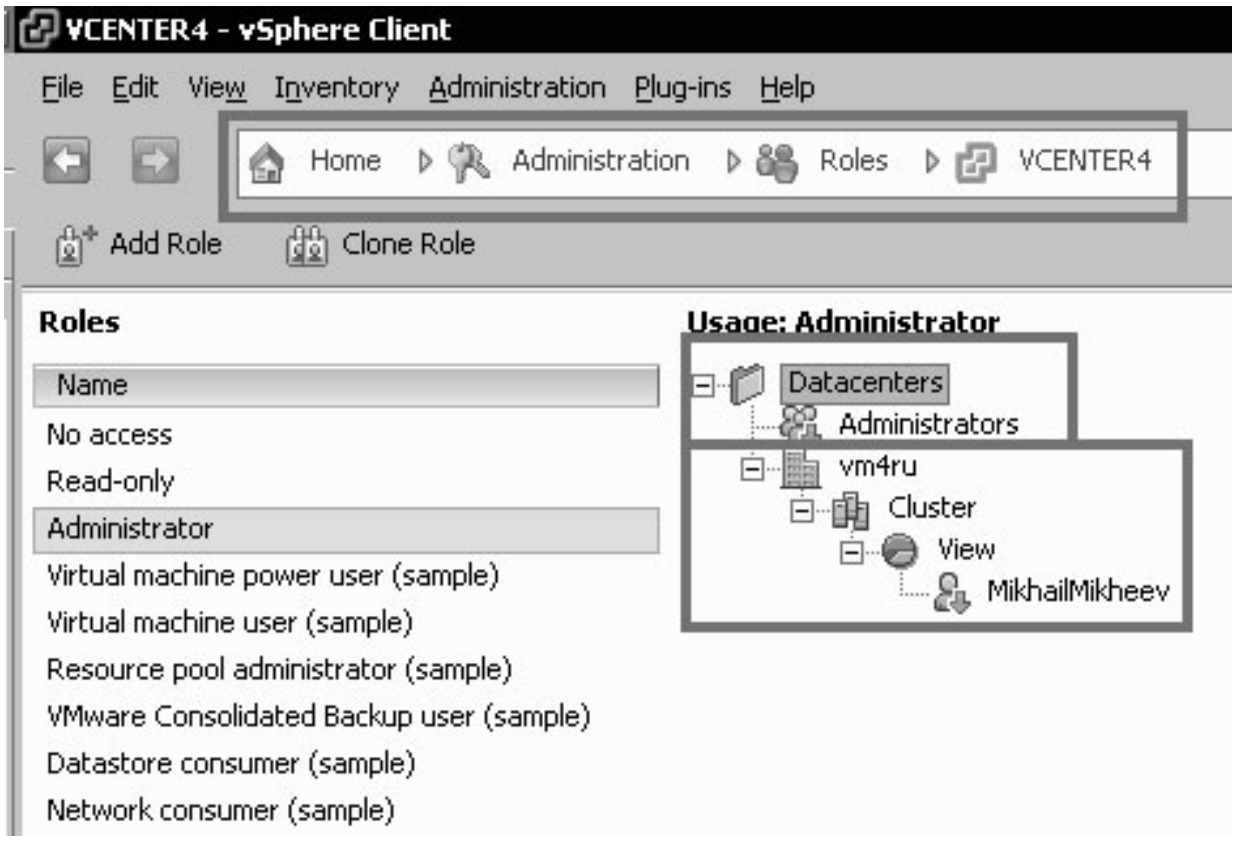


Рисунок 39 Информация о том, на какой уровень иерархии и какому пользователю назначена выбранная роль

Здесь видно, что роль Administrator (слева) дана группе Administrators на уровне объекта Datacenters (самом верхнем уровне иерархии vCenter). Это настройки по умолчанию – группа локальных администраторов на сервере vCenter имеет все права на всю иерархию. Кроме того, здесь эта роль выдана пользователю на пул ресурсов под названием «View».

У vCenter нет собственной БД пользователей, он пользуется:

- локальными пользователями и группами Windows, созданными на сервере, на котором установлен vCenter;
- доменными пользователями и группами того домена, в который входит сервер vCenter (если он в домен входит).

Таким образом, порядок действий для выдачи каких-то прав пользователю или группе следующий:

1. Создается пользователь/группа, если они еще не существуют. Они могут быть локальными в Windows vCenter или доменными, если он входит в домен.
2. Создается роль. Для этого по пути Home Administration Roles. Затем:

• в контекстном меню пустого места выбирается пункт Add для создания новой роли с нуля;

• в контекстном меню существующей роли выбирается пункт Clone для создания копии существующей роли. Если нужно поменять созданную роль, вызывается для нее контекстное меню и выбирается Edit.

Чекбоксами отмечается все необходимые привилегии.

3. Затем Home Inventory и выбирается:

• Hosts and Clusters для раздачи прав на видимые в этой иерархии объекты – кластеры, серверы, каталоги с серверами, пулы ресурсов и др.;

• VMs and Templates – на ВМ, шаблоны и каталоги с этими объектами;

• Datastore – для раздачи прав на хранилища;

• Networking – для раздачи прав на вКоммутаторы.

Как показано на рисунке 40.

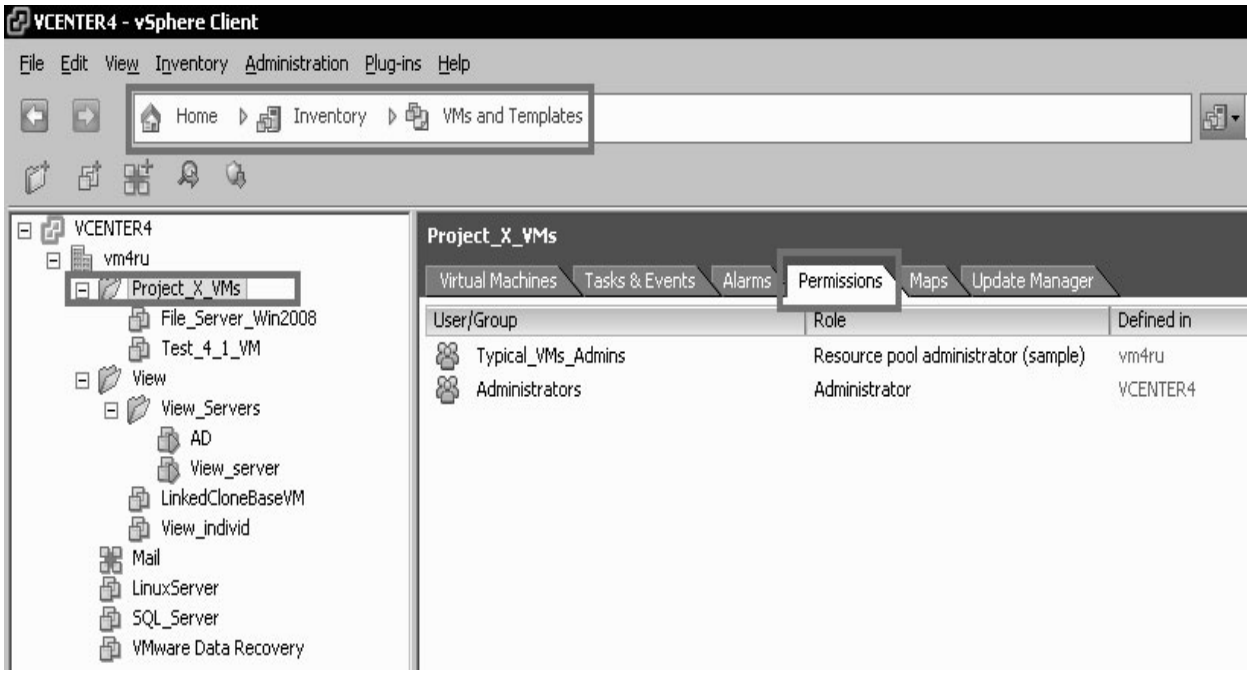
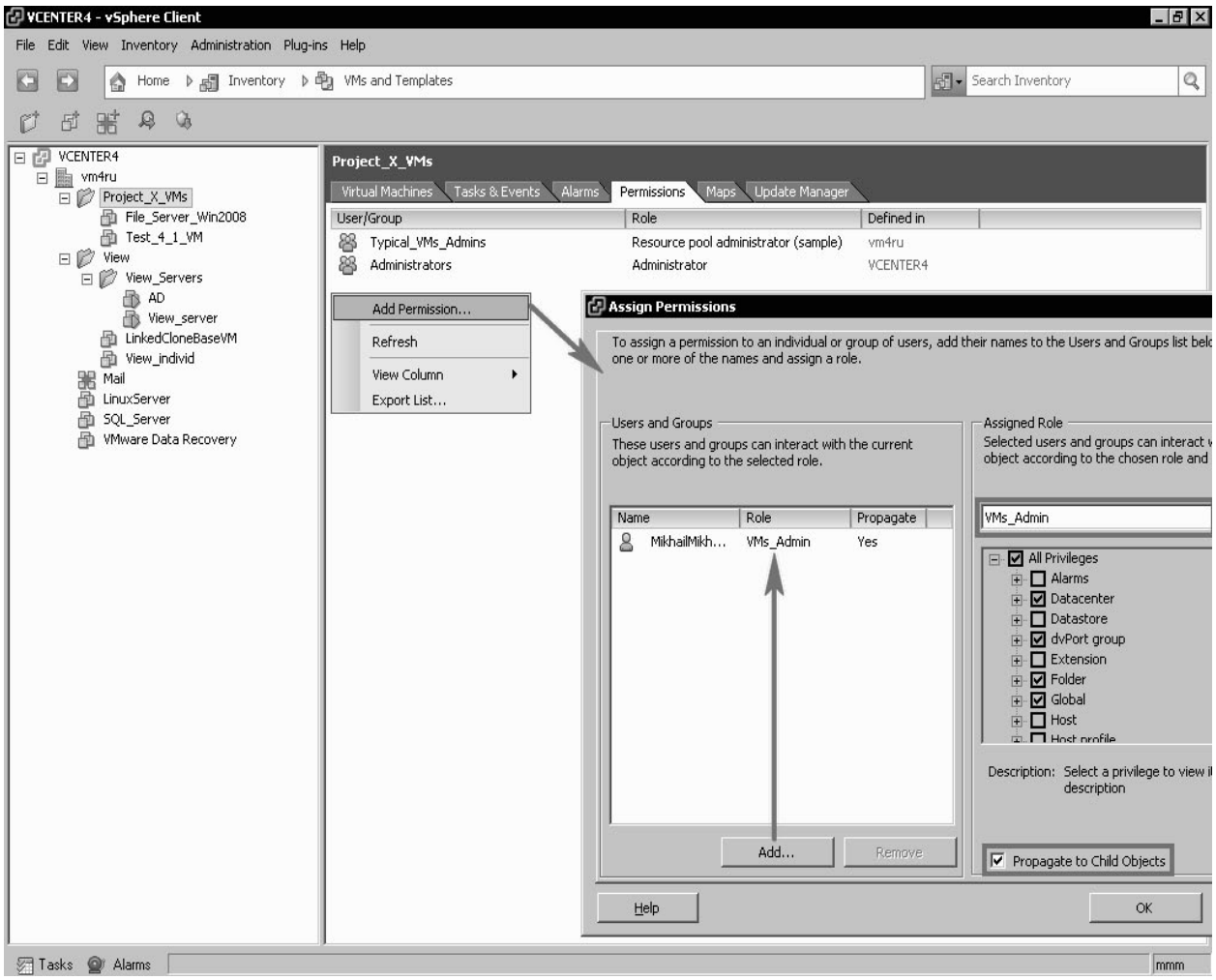


Рисунок 40 - Просмотр разрешений для выбранного объекта

Здесь видимы каталоги для ВМ (они голубого цвета и видны только в режиме «VMs and Templates»). Если перейти на закладку Permissions, будет видна информация о том, кто и какие права имеет сейчас на выбранный объект.

В данном примере видно, что группа Administrators имеет права роли Administrator, притом эта роль назначена группе на уровне «vcenter4» (то есть в корне иерархии vCenter, у меня vcenter4 – это имя машины с установленным vCenter). Кроме того, группе «Typical_VMs_Admins» назначена роль «Resource pool administrator (sample)» на уровне «vm4ru» (в данном примере это название объекта Datacenter, содержащего все серверы и ВМ).

Теперь необходима дать некие права группе или пользователю на объект в иерархии. Оставаясь на закладке Permissions этого объекта, вызывается контекстное меню и выбираем Add Permissions (рисунок 41).



Риунокс. 41- Назначение роли на каталог с ВМ

В открывшемся окне нажатием кнопки Add выбираются пользователи

и группы, затем в правой части из выпадающего меню выбирается роль, которую необходимо им задать. Желаемая роль к этому моменту должна быть создана, делается это в меню Home Administration Roles.

Следует обратить внимание на флажок Propagate to Child Objects (применять к дочерним объектам). Если он не стоит, то права выдаются только на объект (каталог Project_X_VMs), но не на ветвь его подобъектов.

В этом примере было дано пользователю (созданному в Win dows, на которой установлен vCenter) роль VMs_Admin (которая была

создана в vCenter) на каталог Project_X_VMs. Если теперь обратиться клиентом vSphere от имени этого пользователя, то будет видно следующую картину, рисунок - 4.11.

Пользователь не видит других объектов, кроме тех, на которые имеет права, – то есть двух ВМ. Если он просматривает списки событий (Events), то ему доступны события только этих двух объектов. Ему недоступно назначение ролей, недоступно управление лицензиями, и далее, и далее.

Далее немного правил применения прав.

Самое важное: если пользователю выданы разные права на разных уровнях

иерархии vCenter, то результирующими для какого-то объекта являются первые встреченные снизу вверх – рисунок. 42.

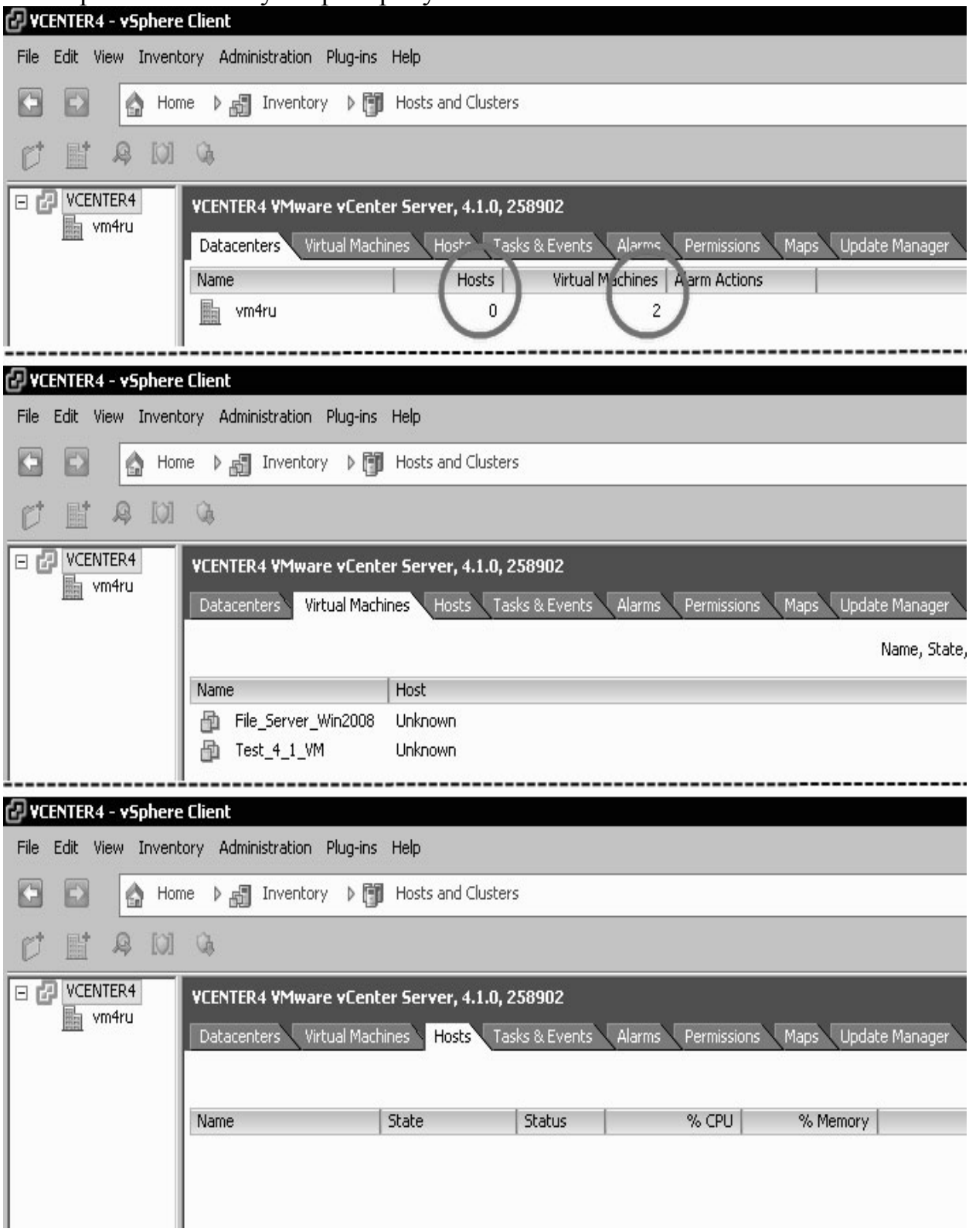


Рисунок. 42 Подключение от имени непривилегированного пользователя

Это достаточно типичная ситуация: пользователь VasilyPupkin имеет роль администратора (то есть все права) на всю иерархию. На пул ресурсов nonCritical_Production_VMs выданы ограниченные права группе

пользователей, в которую входит и VasilyPupkin. По правилам распространения привилегий vCenter, для этого пула и для входящих в него ВМ пользователь не обладает правами администратора, только правами на чтение (рисунок 43).

Ситуацию типичная, потому что не исключено, что администратор будет давать каким-то группам пользователей ограниченные права на группы ВМ (или сетей, или хранилищ. Впрочем, ВМ более вероятны). И бывает,

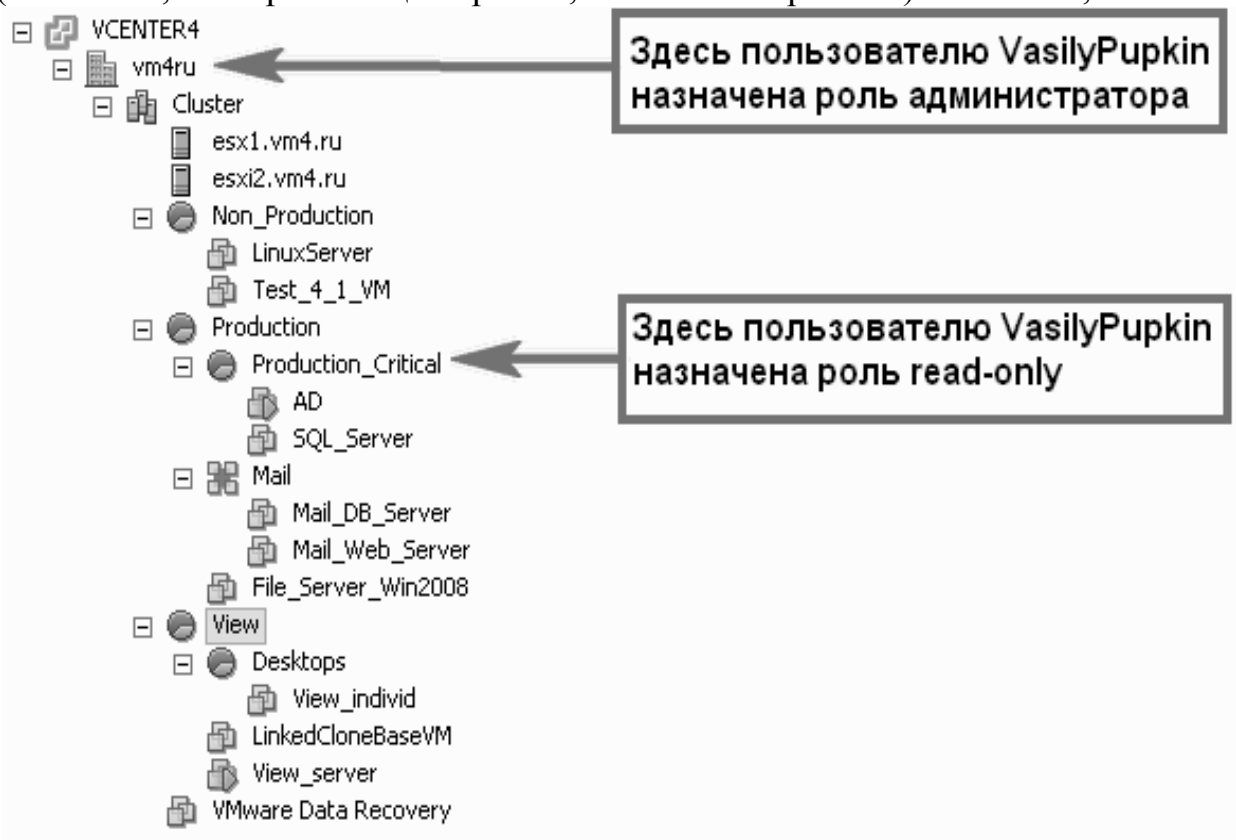


Рисунок - 43. Иллюстрация варианта назначения разных прав на разные уровни иерархии.

Администратор сам входит, или начинает входить через какое-то время, в эту самую группу. И вследствие этого теряет административные привилегии на ветвь иерархии.

Другой случай – на рисунок. 44.

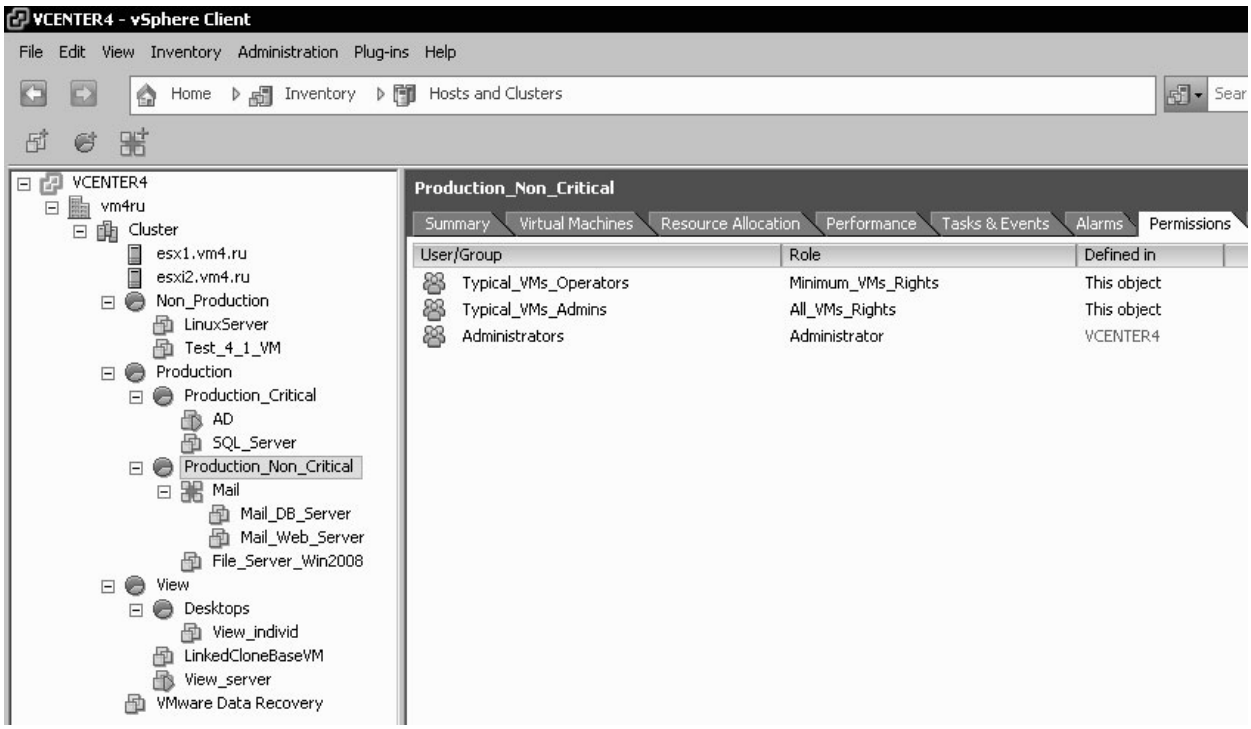


Рисунок. 44. Иллюстрация выдачи разных прав двум группам на один объект иерархии

Здесь видно, что на один и тот же объект в иерархии выданы разные права двум группам. Какие права будут действовать в случае, если мы входим в обе группы? В данном случае происходит объединение привилегий – мы будем обладать теми, что входят хотя бы в одну роль.

Последний пример на рис. 45.

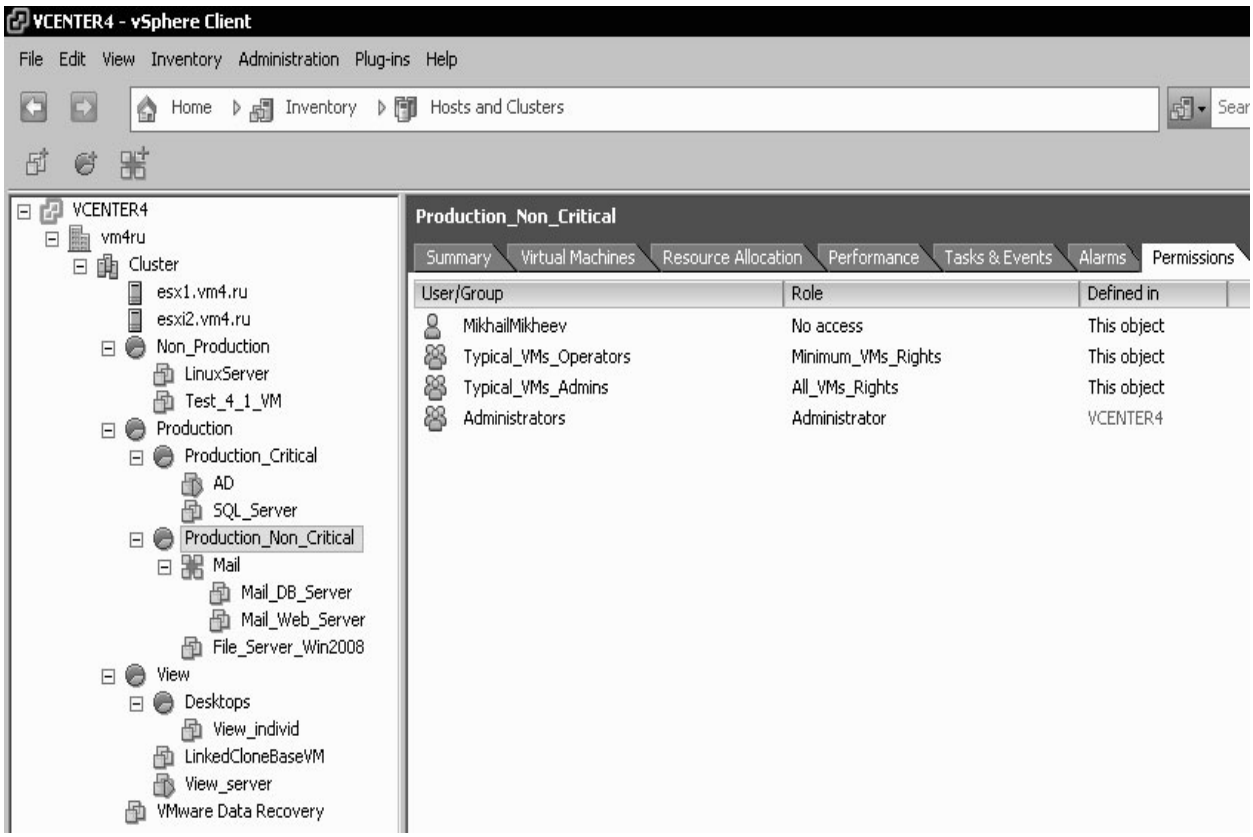


Рисунок 45 - Выдача разных прав пользователю и группе, в которую он входит, на один объект

Здесь на один объект в иерархии выданы права и непосредственно пользователю, и группам, в которые он входит. В данном случае результирующими являются только те права, что выданы непосредственно пользователю.

В данном примере это роль «No access». Эта существующая по умолчанию роль необходима, для явного лишения доступа. Общие соображения по разграничению прав доступа.

Если в компании один администратор, то, скорее всего, вам система раздачи прав не пригодится или пригодится очень ограниченно – на уровне предоставления прав на некоторые ВМ некоторым группам пользователей.

А вот если с разными областями виртуальной инфраструктуры должны работать разные группы администраторов, операторов и пользователей, то имеет смысл сделать примерно так:

1. Составьте перечень повседневных задач, которые придется решать. Если

что-то забудете – ничего страшного, выполните несколько итераций.

Безопасность

Расширенные настройки, безопасность, профили настроек

2. Перечислите, какие объекты иерархии и элементы интерфейса используются для выполнения каждой задачи из списка, составленного выше. Про каждую, и подробно.

3. Распишите, кто и где будет это выполнять.

Полученный в результате документ называется «матрицей доступа к информации». Кто, куда, зачем. Фактически это – основа внутренней документации по безопасности виртуальной инфраструктуры, на ее основе будут создаваться роли и выдаваться на те или иные уровни иерархии, с ее помощью будут фиксироваться изменения. Наличие документации, куда вносятся изменения в конфигурации, является обязательным – иначе вы рискуете в какой-то момент запутаться вплоть до потери доступа к инфраструктуре.

Не используем роли, существующие в vCenter по умолчанию. За исключением роли Administrator (то есть все права), Read-only (просмотр информации об объекте) и No Access (явное отсутствие доступа). Прочие существующие по умолчанию роли использовать не рекомендуется (кроме роли VMware Consolidated Backup user (sample)).

Само собой, правильным будет создание ролей под конкретные нужды, а не использование одной роли, которая может все. Создаем роли под конкретные задачи с минимально необходимым набором прав. Существующие по умолчанию роли не соответствуют этому условию.

Однозначно роли должны назначаться персонифицированно, то есть не должно быть учетной записи, из-под которой могут аутентифицироваться несколько человек. Это чрезвычайно помогает, в частности если необходимо восстановить последовательность событий и виновное лицо.

Не используются локальные учетные записи, кроме исключительных случаев. Только доменные. Тем более это удобнее – для аутентификации в vSphere можно использовать ту учетную запись, от имени которой был выполнен вход в Windows, и не набирать пароль заново.

Настройках по умолчанию: локальная группа администраторов

имеет все права на корень иерархии vCenter. Конечно же правильно будет:

1. Создать персонифицированную учетную запись (даже две).
2. Наделить их правами администратора на все в vCenter.
3. Убрать их данные в сейф, пользоваться ими лишь в исключительных случаях.
4. Лишить группу локальных администраторов прав в vCenter.

6.3 Настройка сертификатов SSL

VMware vSphere, а именно продукты ESX(i) 4, vCenter 4, VMware Converter Enterprise и VMware Update Manager 4, поддерживают SSL v3 и TLS v1 (обычно употребляется просто «SSL»). Если SSL включен, то трафик между узлами виртуальной инфраструктуры зашифрован, подписан и не может быть незаметно изменен. ESX(i), как и другие продукты VMware, использует сертификаты X.509 для шифрования передаваемого по SSL трафика.

В vSphere 4 проверка сертификатов включена по умолчанию, и они используются для шифрования трафика. Однако по умолчанию эти сертификаты генерируются автоматически во время установки ESX(i). Эта процедура не требует от администратора каких-то действий. Но они не выданы центром сертификации (certificate authority, CA. Также иногда упоминается в русскоязычной документации как «удостоверяющий центр», УЦ). Такие самоподписанные сертификаты потенциально уязвимы для атак «человек в середине». Потому что для них до того, как начинается шифрование трафика, не производится проверка подлинности самих сертификатов.

При попытке подключения к ESX(i) или vCenter (с помощью клиента

vSphere или браузера) пользователю выдается соответствующее предупреждение (рисунок 46), сообщающее ему о том, что удаленная система может не являться доверенной и установить ее подлинность не представляется возможным. Конечно, это предупреждение можно отклонить, можно занести сертификаты всех управляемых систем в список доверенных, но это может ослабить безопасность инфраструктуры. К тому же, возможно, в вашей организации запрещено использование систем с недоверенными сертификатами (административно или технически).

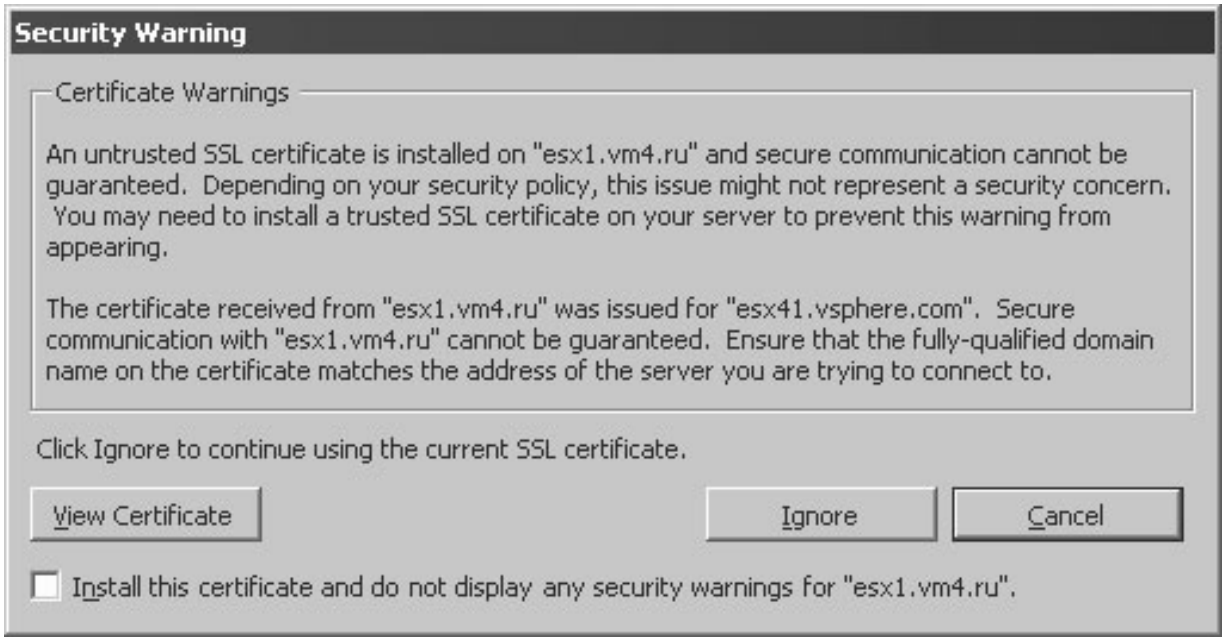


Рисунок. 46. Предупреждение о недоверенном сертификате

Для решения этих проблем вам потребуется запросить у доверенного центра сертификации подходящий сертификат и заменить им сгенерированные автоматически. Доверенный центр сертификации может быть коммерческим (например, VeriSign, Thawte или GeoTrust) или установленным в вашей сети (например, Microsoft Windows Server Active Directory Certificate Cervices, AD CS или OpenSSL).

Примерный план этого действия выглядит следующим образом.

1. Получение сертификата для ESX(i), замена ими сгенерированных по умолчанию сертификатов.

2. Получение сертификатов для vCenter 4 и Update Manager 4. Замена сгенерированных по умолчанию сертификатов. Обратите внимание на то, что замена сертификата для уже установленного Update Manager возможна лишь

Настройка сертификатов SSL

Расширенные настройки, безопасность, профили настроек

с его переустановкой. Это связано с тем, что он хранит свои сертификаты в

своем собственном формате, конвертация в который происходит при установке продукта.

Здесь не приводятся конкретные инструкции, так как они сильно зависят от вашей инфраструктуры, да и далеко не всем администраторам vSphere придется заниматься этим вопросом.

6.4 Выводы по третьей главе

Внедрение виртуализации позволило на практике убедиться во всех преимуществах, предлагаемых данной технологией. Консолидация серверов значительно снизила общую стоимость оборудования, расходы на электроэнергию и обслуживание.

Виртуализация приложений позволила ускорить процесс развертывания клиентских программ на рабочие станции, упростить их обслуживание, сделать процесс более гладким и быстрым.

Повысилась отказоустойчивость серверов, время простоя при сбое сократилось до минимума. Благодаря возможности делать снимки, восстановление практически любого сервера и виртуальной машины является делом нескольких минут.

ЗАКЛЮЧЕНИЕ

Внедрение виртуализации позволило на практике убедиться во всех преимуществах, предлагаемых данной технологией. Консолидация серверов значительно снизила общую стоимость оборудования, расходы на электроэнергию и обслуживание.

Виртуализация приложений позволила ускорить процесс развертывания клиентских программ на рабочие станции, упростить их обслуживание, сделать процесс более гладким и быстрым.

Повысилась отказоустойчивость серверов, время простоя при сбое сократилось до минимума. Благодаря возможности делать снимки, восстановление практически любого сервера и виртуальной машины является делом нескольких минут.

В ходе данной диссертации удалось наглядно выяснить все преимущества технологии виртуализации и ее удобство, и необходимость в процессе обучения IT специалистов, системных администраторов и специалистов в области баз данных. Благодаря успешно проведенному эксперименту в компании ТОО Каисса удалось наглядно увидеть преимущества применения данной технологии. В заключении предлагаю для нашего института приобрести собственный кафедральный сервер, который позволит создать внутреннюю кафедральную сеть, и использовать его для дальнейшего обучения студентов, т.к. самые эффективные занятия – это те, где для студента есть возможность «потрогать» без страха, что возможно, что – то сломается.

(1на страница полностью!!!!!!!!!!!!!!!!!)

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 (нумерация без точек) Tulloch M. Understanding Microsoft Virtualization Solutions, From the Desktop to the Datacenter, 2nd Edition – Redmond: Microsoft Press, 2010. – 464 с.

2. Kelbley J., Sterling M. Windows Server 2008 R2 Hyper-V: Insiders Guide to Microsoft's Hypervisor. – Indianapolis: Wiley Publishing, Inc., 2010. – 385 с.

3. Minasi M., Gibson D., Finn A., Henry W., Hynes B. - Mastering Windows Server 2008 R2. – Indianapolis: Wiley Publishing, Inc., 2010. – 1454 с.

4. Михеев М. - Администрирование VMware vSphere 4.1 (Администрирование и защита) 2012, - 236 с.

5. ru.wikipedia.org/wiki/ Интернет энциклопедия статья Гипервизор

6. http://lvee.org/en/reports/LVEE_2011_20 статья, посвященная истории развития технологии VMware (дата обращения: 12.12.12)

7. Интернет портал «PC MAGAZINE» статья, посвященная истории виртуализации http://www.pcmag.ru/elearning/course/lesson. php?COURSE_ID=14&ID=106

8. lib.znate.ru/docs/index-6533.html Информационный портал, статья на тему Сети

9. habrahabr.ru информационный портал статья, посвященная теме виртуализация Hyper-v, сети типа vlan.

10. ru.wikipedia.org/wiki/ Интернет энциклопедия статья на тему Система виртуальных машин

11. bestreferat.ru/referat-105014.htlm Реферат на тему История и особенности развития беспроводного доступа

12. osp.ru/text/print/302/184272.html научная статья на тему особенности технологии виртуализации

13. window.edu.ru/resource/848/62848/files/tm2008.html статья на тему применение технологии виртуализации

14. http://library.by/portalus/modules/computers/print.php?archive= &id=1237562305&start_from=&subaction=showfull&ucat Статья на тему технологии виртуализации

15. http://www.e-reading.org.ua/download.php?book=135150 Станек Microsoft SQL Server 2005 Справочник администратора.г.

16. Максим Л. Технология Виртуализации. 2013, - 403 с.

17. WILEY - MASTERING VMWARE INFRASTRUCTURE 3 2010 г.

18. Windows Server 2008 HYPER-V. Insider's guide to microsoft hypervisor (sybex 2009)

19. Rand Morimoto и Jeff Gullet Windows Server 2008 Hyper-V UNLEASHED

20. Harley Stagner Pro Hyper-V. (Apress 2009), 2009, - 401 с. (образец)

21. Microsoft MSPress Windows Server 2008 Terminal Services Resource Kit