Ставропольский государственный аграрный университет

А.И. Сосин

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Лабораторный практикум

Ставрополь

СОДЕРЖАНИЕ

Введение

Сегодня присутствие средств вычислительной техники и использование информационных систем (ИС) в жизни и деятельности человека стало повсеместным. Стали повсеместными и проблемы управления или администрирования информационных систем. Необходимость в специалистах, которые умеют это делать профессионально, очевидна. При этом потребность в них возрастает, а область их деятельности постоянно расширяется с увеличением размеров и сложности информационных систем.

В учебном пособии содержатся некоторые практические рекомендаций по различным вопросам администрирования систем, и оно будет полезно студентам при изучении курса администрирования в ИС.

Дисциплина «Администрирование в ИС» является завершающей в подготовке студента, и в ней излагаются общие методы администрирования ИС.

Конкретные вопросы конфигурирования и параметризации программных и аппаратных средств, программирования ИС и систем управления, защиты информации ИС, диагностики и метрологии ИС детально рассматриваются в ряде дисциплин, предшествующих этому курсу.

Лабораторная работа № 1

СОЗДАНИЕ И АДМИНИСТРИРОВАНИЕ ХРАНИЛИЩ ДАННЫХ

Цель работы: изучить основы и освоить практически консольный и классический способы управления процессом подготовки аппаратных и программных средств, требуемых для Windows Server 2012, освоить способы организации хранилищ данных под управлением серверных платформ.

Основные сведения

Планирование установки сервера

Прежде чем приступать к самому процессу установки Windows Server 2012, необходимо сначала принять несколько решений относительно предшествующих ему шагов.

Минимальные требования к оборудованию

Перед установкой Windows Server 2012 как в лабораторной, так и в производственной среде необходимо удостовериться, что выбранное оборудование отвечает минимальным требованиям к системе. В большинстве ситуаций соответствия оборудования официальным минимальным требованиям далеко недостаточно. Поэтому в табл.1 перечислены не только минимальные, но также рекомендуемые и максимальные требования к системе для различных компонентов оборудования.

Таблица 1

Системные требования для установки ОС Windows Server 2012

Компонент	Минимальные требования	Рекомендуемые требования	Максимальные требования
Процессор	*1,4 ГГц, 64-разрядная архитектура*	*2 ядра по 2 ГГц или более*	*Отсутствуют*
ОЗУ	*512 МБ*	*2 ГБ и более*	*32ГБ для Standard Edition и 4ТБ для Datacenter Edition.*
Свободное место на диске	*32 ГБ*	*40 ГБ для полной установки или 10 ГБ для Server Core*	*Отсутствуют*

При проектировании и выборе технических характеристик системы для нового серверного решения даже предлагаемых Microsoft оптимальных требований к системе может оказаться недостаточно. Поэтому рекомендуется оценивать характеристики сервера для выбранной серверной роли с учетом нагрузки во время развертывания и возможности ее увеличения в будущем. Например, системе на базе Windows Server 2012 с ролью Exchange Server 2010 Mailbox Server (Сервер почтовых ящиков Exchange Server 2010) или SQL Server 2012 для решений бизнес-логики уровня предприятия для нормальной работы потребуется гораздо более 2ГБ ОЗУ. Поэтому обязательно должным образом оценивайте размер системы и тестируйте ее нагрузку перед переносом в производственную среду.

В Windows Server 2012 поддерживается использование процессоров только с 64-разрядной архитектурой. Серверы, работающие под управлением процессоров с 32-разрядной архитектурой, больше не поддерживаются.

Описание служебной программы Diskpart с интерфейсом командной строки

Отличие программы Diskpart от многих других служебных программ с интерфейсом командной строки заключается в том, что она выполняется не в однострочном режиме, а считывает команды из стандартного ввода-вывода. Такие команды могут относиться к любому диску, разделу или тому. Вызвать консоль PowerShell можно сочетанием клавиш Shift+F10.

Сравнение с оснасткой "Управление дисками"

Программа Diskpart позволяет выполнять расширенный набор действий, поддерживаемых оснасткой "Управление дисками". Оснастка "Управление дисками" защищает данные на диске путем блокирования действий, которые могут привести к их повреждению. Будьте внимательны, используя программу Diskpart, поскольку она предоставляет явный контроль над разделами и томами!

Программа Diskpart позволяет преобразовать базовый диск в динамический. При этом базовый диск может быть пустым, содержать основные разделы или логические диски, являться диском с данными, системным или загрузочным диском, но не должен иметь в своем составе отказоустойчивых наборов (FtDisk), например, чередующихся или зеркальных наборов. Для преобразования базовых дисков, которые содер-

жат наборы FtDisk, следует использовать оснастку "Управление дисками" из состава Windows 2000 или преобразовать диск перед обновлением до Windows XP.

С помощью программы Diskpart можно преобразовать динамический диск в базовый. До начала преобразования необходимо удалить все динамические тома. Кроме случаев крайней необходимости, удалять разделы на динамических дисках не рекомендуется. Перед преобразованием диска в базовый рекомендуется удалить на нем все тома. Удалите все динамические разделы с данными. Не используйте динамические разделы и основной базовый раздел на одном диске — в этом случае компьютер может не загрузиться.

Программа Diskpart позволяет создавать на диске разделы со смещением. Оснастка "Управление дисками" всегда размещает раздел в конце любой занятой области или первой обнаруженной области достаточного размера. На дисках с основной загрузочной записью (MBR) смещение и размер раздела округляются для сохранения требуемой конфигурации цилиндров до ближайшего действительного значения (размер — с повышением). Программа Diskpart не присваивает букву диска созданному разделу. Назначить букву диска или точку подключения можно с помощью команды assign.

Подобно оснастке "Управление дисками", программа Diskpart создает динамические диски только на несъемных жестких дисках и не позволяет преобразовывать съемные диски (например, диски USB или 1394) в динамические.

С помощью программы Diskpart можно выполнить некоторые операции по удалению разделов, которые блокируются оснасткой "Управление дисками" (например, удалить MBR-диск OEM). Однако такие разделы часто содержат файлы, необходимые для обеспечения работы платформы в целом. Программа Diskpart блокирует удаление текущих системных и загрузочных томов и разделов, томов и разделов, содержащих файл подкачки, а также разделов, которые лежат в основе динамических дисков.

С помощью программы Diskpart невозможно создать раздел на съемном носителе. Операционные системы Windows поддерживают на съемных носителях не более одного раздела с MBR. Если носитель изготовлен с основной загрузочной записью, ее невозможно изменить, однако эта запись соблюдается, даже если настроено несколько разделов или логических дисков. В противном случае, если носитель изготовлен без основной загрузочной записи, он рассматривается в качестве диска в формате "superfloppy" и не содержит структуры разделов.

Буква сопоставляется не самому съемному носителю, а диску и может быть изменена с помощью программы Diskpart.

Запуск программы Diskpart приводит к созданию подписей дисков, идентификаторов GUID для дисков с таблицей разделов GPT и для GPT-разделов, однако эти значения невозможно установить явно.

Подобно оснастке "Управление дисками", программа Diskpart поддерживает новую схему Itanium разбиения дисков на разделы под названием GPT. GPT-диски не могут быть использованы на компьютерах с архитектурой x86 под управлением Windows XP или Windows 2000. Программа Diskpart позволяет преобразовывать разбиение диска по схеме GPT в формат MBR только на пустых дисках.

С помощью программы Diskpart можно удалять отсутствующие динамические диски. Динамические диски содержат в своем составе общую базу данных, и поэтому каждый динамический диск имеет сведения об остальных динамических дисках на конкретном компьютере. В случае перемещения динамического диска исходный компьютер считает его отсутствующим.

Программа Diskpart не назначает буквы дисков для разделов и томов автоматически — это необходимо сделать вручную, указав букву самостоятельно или приняв следующую доступную букву.

Установка фокуса

Большинство команд Diskpart выполняются по отношению к определенному диску, разделу или тому. Такой целевой объект находится "в фокусе". Установка фокуса упрощает выполнение стандартных задач настройки, предполагающих создание нескольких разделов на одном диске. Для помещения объекта в фокус служит команда select. Установка фокуса требуется для выполнения всех команд (за исключением list, rem, exit и help).

Чтобы переместить фокус явно, используется команда select. Кроме того, с помощью некоторых команд, например, create, это может быть сделано неявно. Перед выполнением действий с базовым диском необходимо переместить на него фокус. На базовом диске выбранный раздел и выбранный том — это одно и то же. Перемещение одного из фокусов автоматически приводит к перемещению фокуса другого объекта. На динамическом томе значение имеет только фокус тома, поскольку предыдущий фокус раздела всегда теряется, а фокус диска важен только для простых томов.

Сценарии

Программа Diskpart поддерживает выполнение сценариев. Для запуска сценария служит команда *diskpart /s script.txt*. Сценарии Diskpart могут быть запущены в среде Windows XP, Windows 2000, в случае автоматической установки с помощью служб удаленной установки (RIS), а также в среде предварительной установки Windows для OEM.

По умолчанию программа Diskpart прерывает обработку команд и возвращает код ошибки в случае возникновения проблемы с выполнением сценария. Чтобы изменить такое поведение (сценарий продолжает выполняться даже после появления ошибки), необходимо включить в команду параметр *noerr*. Это параметр позволяет с помощью одного сценария удалить все разделы на всех дисках с данными, независимо от общего числа дисков. Однако параметр *noerr* поддерживается не всеми командами. Кроме того, даже если используется параметр *noerr*, код ошибки возвращается в случае наличия ошибки в синтаксисе команды.

Коды ошибок, возвращаемые программой Diskpart:

0. успешное завершение операции, сценарий выполнен без ошибок;

1. неустранимая ошибка, возможны серьезные неполадки;

2. в командной строке Diskpart указаны неверные аргументы;

3. программе DiskPart не удалось открыть указанный сценарий или выходной файл;

4. сбой в одной из служб, использованных программой DiskPart;

5. ошибка в синтаксисе команды, сценарий не выполнен, поскольку объект выбран неправильно или не может быть использован с данной командой.

После выполнения программы Diskpart отображается ее версия и текущее имя компьютера.

Обзор команд

Перемещение фокуса на объект:

select

Команда select служит для установки фокуса на определенный объект. Чтобы отобразить список типов фокусов, запустите команду select без параметров. Если не указать идентификатор, будет отображен текущий выбранный объект.

select disk[=n]

Команда select disk служит для помещения в фокус диска Windows NT с указанным номером. Если не указать номер диска, будет отображен текущий выбранный диск.

select partition[=n/l]

Команда select partition служит для установки фокуса на определенный раздел. Если не указать раздел, будет отображен текущий выбранный раздел.

На базовом диске раздел можно указать по индексу, букве диска или точке подключения, а на динамическом диске — только по индексу.

select volume[=n/l]

Команда select volume служит для перемещения фокуса на указанный том. Если том не указан, отображается текущий том в фокусе.

Том можно указать по индексу, букве диска или пути к точке подключения. При выборе тома на базовом диске фокус перемещается на соответствующий раздел.

Отображение конфигурации дисков

Для получения общих сведений служит команда list, а чтобы отобразить более подробную информацию, установите фокус и воспользуйтесь командой detail.

detail disk - вывод подробной информации о диске в фокусе.

detail partition - вывод подробной информации о разделе в фокусе.

detail volume - вывод подробной информации о томе в фокусе.

list disk

Команда list disk служит для получения общих сведений о каждом установленном на компьютере диске. Диск, отмеченный звездочкой (*), находится в фокусе. Перечисляются только жесткие (например, стандарта IDE и SCSI) и съемные (например, стандарта 1394 и USB) диски.

list partition

Команда *list partition* служит для получения сведений о каждом разделе на выбранном диске. Отображаются все разделы, независимо от типа.

list volume

Команда *list volume* служит для получения сведений о каждом томе на компьютере.

Управление базовыми дисками:

На MBR-дисках параметры *size* и *offset* округляются в соответствии с конфигурацией цилиндров. На GPT-дисках параметры size и offset округляются в соответствии с конфигурацией секторов. Если параметр offset не указан, раздел размещается в первой непрерывной незанятой области, имеющей достаточный размер. Если параметр size не указан, раздел может занять все пространство на выбранном диске.

При первом обнаружении новые диски считаются MBR-дисками. Перед созданием раздела GPT диск необходимо явно преобразовать в

формат GPT. MSR-раздел рекомендуется создавать первым на диске с данными и вторым (после ESP) на системном или загрузочном диске. После преобразования MBR-диска в формат GPT MSR-раздел создается автоматически.

Фокус всегда перемещается на созданный раздел. Удаление любого раздела приводит к потере фокуса. Фокус диска в любом случае не меняется.

active

Пометка имеющего фокус раздела на базовом диске как активного. Эта информация указывает встроенному ПО, что раздел является действительным системным разделом. Программа DiskPart не проверяет содержимое раздела.

Примечание. В результате неправильного использования этой команды компьютер может не загрузиться.

assign [[letter=l]/[mount=путь]] [noerr]

Назначение буквы диска или точки подключения разделу в фокусе. Если буква диска не указана, используется следующая доступная буква. Если буква диска или точка подключения уже используются и не указан параметр noerr, возникает ошибка. Команда может быть использована для изменения буквы, назначенной съемному носителю. Нельзя назначить букву диска системному тому, загрузочному тому или тому, который содержит файл подкачки. Кроме того, буква диска не может быть назначена OEM-разделу или GPT-разделу, отличному от раздела Msdata.

create partition primary [size=n] [offset=n] [id=байт/guid] [noerr]

Создание на текущем диске основного раздела указанного размера и с указанным смещением начального адреса. Если байт ИД раздела на MBR-диске не задан, команда создает раздел типа 0x6. Параметр ID служит для указания типа раздела. Проверка допустимости байта типа раздела или другие проверки параметра ID не производятся. Если идентификатор GUID типа раздела на GPT-диске не задан, команда создает раздел MSDATA. С помощью параметра ID может быть задан любой идентификатор GUID. Команда DiskPart не выполняет проверку на допустимость, уникальность (или иную проверку) идентификатора GUID. Идентификатор GUID экземпляра раздела создается автоматически. Операционная система Windows не назначает буквы дисков созданным разделам MBR и GPT автоматически. Это необходимо сделать самостоятельно.

create partition extended [size=n] [offset=n] [noerr]

Создание на текущем диске дополнительного раздела указанного размера и с указанным смещением начального адреса. Диск должен иметь формат MBR. После создания раздела фокус автоматически перемещается на этот раздел. На диске можно создать только один дополнительный раздел. Логические диски могут быть созданы только после дополнительного раздела.

create partition logical [size=n] [offset=n] [noerr]

Создание в существующем дополнительном разделе на текущем диске логического диска указанного размера и с указанным смещением начального адреса. Диск должен иметь формат MBR. Если смещение не указано, логический диск размещается в первой непрерывной незанятой области дополнительного диска, имеющей достаточный размер. Если размер не указан, раздел занимает все свободное пространство дополнительного раздела. После создания раздела фокус автоматически перемещается на новый логический диск.

create partition msr [size=n] [offset=n] [noerr]

Выполнение команды create partition msr равнозначно созданию раздела с идентификатором MSR GUID E3C9E316-0B5C-4DB8-817D-F92DF00215AE.

create partition esp [size=n] [offset=n] [noerr]

Выполнение команды create partition esp равнозначно созданию раздела с идентификатором ESP GUID C12A7328-F81F-11D2-BA4B-00A0C93EC93B.

delete partition [noerr] [override]

Команда delete partition служит для удаления раздела в фокусе. Нельзя удалить системный раздел, загрузочный раздел, а также раздел, содержащий файл подкачки. Чтобы удалить раздел ESP, MSR или известный раздел OEM, необходимо указать параметр override.

extend [size=n] [noerr]

Расширение тома в фокусе на смежное невыделенное пространство. Невыделенная область должна находиться на том же диске и следовать (иметь более высокое смещение) за разделом в фокусе. С помощью этой команды существующий базовый раздел данных может быть расширен за счет созданного пространства массива RAID. Если раздел был ранее отформатирован с использованием файловой системы NTFS, файловая система автоматически расширяется на увеличенный раздел без потери существующих данных. Если раздел был ранее отформатирован с ис-

пользованием другой файловой системы (отличной от NTFS), выполнение команды завершается неудачно (и без изменения раздела). Невозможно расширить текущий системный или загрузочный разделы.

remove [[letter=l]/[mount=путь]/[all]] [noerr]

Удаление буквы диска или точки подключения для раздела в фокусе. Если используется параметр *all*, удаляются все текущие буквы дисков и точки подключения. Если буква диска или точка подключения не указаны, удаляется следующая доступная буква. Команда может быть использована для изменения буквы, назначенной съемному носителю. Не допускается удаление буквы диска для системного и загрузочного тома, а также для тома, содержащего файл подкачки. Кроме того, не допускается удаление букв диска OEM-разделов, любых GPT-разделов с нераспознанным идентификатором GUID, а также специальных не содержащих данных GPT-разделов, например разделов ESP.

Управление динамическими дисками:

Рассмотренные в этом разделе команды используются для создания и удаления томов, восстановления отказоустойчивых томов, а также для импорта дисков. Значение параметра *size* округляется в МБ. Указать смещение нельзя. Том всегда размещается в первой непрерывной незанятой области диска, имеющей достаточный размер. Если размер не указан, создается том максимально возможного размера. Фокус перемещается на созданный том. Если том располагается на нескольких дисках, текущий фокус диска теряется. Удаление тома приводит к потере фокуса тома. Если фокус диска был установлен перед удалением тома, он сохраняется.

Примечание. Программа Diskpart создает MSR-раздел на каждом пустом диске, который преобразуется в динамический диск или в формат GPT.

active

Пометка имеющего фокус тома как активного. Эта информация указывает встроенному ПО, что раздел является действительным системным разделом. Программа DiskPart проверяет раздел только на допустимость нахождения на нем загрузочного образа операционной системы и не проверяет содержимое раздела. В результате неправильного использования этой команды компьютер может не загрузиться.

add disk=n [noerr]

Команда add служит для добавления на указанный диск зеркальной копии тома в фокусе. Поддерживается только две зеркальных копии. Выбранный том должен быть простым томом.

assign [[letter=l]/[mount=путь]] [noerr]

Назначение буквы диска или точки подключения тому в фокусе. Если буква диска не указана, используется следующая доступная буква. Если буква диска или точка подключения уже используются и не указан параметр noerr, возникает ошибка. Нельзя назначить букву диска системному тому, загрузочному тому или тому, который содержит файл подкачки.

break disk=n [nokeep] [noerr]

Разбивает зеркальный том в фокусе. По умолчанию содержимое обеих половин зеркала сохраняется. Каждая половина становится простым томом. Если задан параметр nokeep, сохраняется только указанная половина зеркала, а другая удаляется и преобразуется в свободное пространство. Исходный том сохраняет все буквы диска или точки подключения. Если половина зеркала не сохраняется, фокус остается на оставшемся простом томе на указанном диске. В противном случае фокус перемещается на указанную половину зеркала. Половина зеркала становится простым томом без назначения буквы диска.

create volume simple [size=n] [disk=n] [noerr]

Команда create volume simple служит для создания простого тома указанного размера на определенном диске. Если размер не задан, новый том занимает все свободное место на диске. Если диск не задан, используется диск в фокусе. После создания тома фокус автоматически перемещается на этот том.

create volume stripe [size=n] disk=n[,n[,...]] [noerr]

Команда create volume stripe служит для создания чередующегося тома на указанных дисках. Общий размер чередующегося тома равен указанному размеру, помноженному на число дисков. Если размер не задан, создается чередующийся том максимально возможного размера. Определяется диск с наименьшим доступным непрерывным свободным пространством, в соответствии с размером которого и создается чередующийся том. Пространство такого же размера выделяется на каждом последующем диске.

create volume mirror [size=n] disk=n, n [noerr]

Команда create volume mirror служит для создания зеркального тома на указанных дисках. Общий размер зеркального тома равен указанному размеру. Если размер не задан, создается зеркальный том максимально возможного размера.

create volume raid [size=n] disk=n[,n[,...]] [noerr]

Команда create volume raid служит для создания тома RAID-5 на указанных дисках. На каждом диске выделяется пространство указанного

в параметре size размера. Если размер не указан, создается том RAID-5 максимального возможного размера. Определяется диск с наименьшим доступным непрерывным свободным пространством, в соответствии с размером которого и создается том RAID-5. Пространство того же размера выделяется на каждом диске. Фактический объем доступного дискового пространства на томе RAID-5 меньше суммы занятого дискового пространства, поскольку некоторая его часть требуется для четности.

delete disk [noerr] [override]

Команда delete disk служит для удаления отсутствующего динамического диска из списка дисков. Если параметр override не задан, удаляются все простые тома и половины зеркальных томов на диске. Если часть диска входит в том RAID-5, команда не выполняется.

delete partition [noerr] [override]

Команда delete partition служит для удаления раздела в фокусе. Невозможно удалить разделы, которые содержат существующие подключенные динамические тома. Необходимо предварительно удалить такие тома и преобразовать диск в базовый. Чтобы удалить раздел ESP, MSR или известный раздел OEM, необходимо указать параметр override. Разделы динамических дисков можно только удалять, но не создавать. Например, можно удалить нераспознанный GPT-раздел на динамическом GPT-диске. Доступ к освобожденному после удаления пространству отсутствует. Данная команда позволяет восстановить пространство поврежденного автономного динамического диска в аварийной ситуации, когда нельзя воспользоваться командой clean.

delete volume [noerr]

Команда delete volume служит для удаления тома в фокусе. Выполнение команды приводит к потере всех данных.

extend disk=n [size=n] [noerr]

Команда extend служит для расширения текущего простого или расширенного тома на указанный диск. Команда предназначена для использования только с томами с файловой системой NTFS. Если размер не указан, том может занять все свободное пространство на указанном диске. Существующий фокус диска теряется.

import [noerr]

Команда import служит для импорта всех дисков из внешней группы. Импортируется каждый диск, находящийся в одной группе с диском, имеющим фокус. После выполнения команды текущий фокус диска или тома теряется.

online [noerr]

Подключение отключенного ранее диска или тома. Выполнение команды не приводит к перемещению фокуса.

remove [[letter=l]/[mount=путь]/[all]] [noerr]

Удаление буквы диска или точки подключения тома в фокусе. Если используется параметр all, удаляются все текущие буквы дисков и точки подключения. Если буква диска или точка подключения не указаны, удаляется следующий доступный путь. Не допускается удаление буквы диска для системного и загрузочного тома, а также для тома, содержащего файл подкачки.

retain

Подготовка существующего динамического простого тома к использованию в качестве загрузочного или системного тома. В компьютерах на базе процессоров x86 — создание MBR-раздела на динамическом простом томе, имеющем фокус. Для создания MBR-раздела динамический простой том должен начинаться со смещения, выровненного по цилиндру, а его размер должен быть кратен размеру цилиндра. В компьютерах на базе процессоров Itanium выполнение команды retain приводит к созданию GPT-раздела на динамическом простом томе, имеющем фокус.

Преобразование дисков:

convert mbr [noerr]

Команда convert mbr служит для преобразования стиля разделов текущего диска в формат MBR. Диск может быть базовым или динамическим, но не должен содержать разделов или томов с данными.

Convert gpt [noerr]

Команда convert gpt служит для преобразования стиля разделов текущего диска в формат GPT. Диск может быть базовым или динамическим, но не должен содержать разделов или томов с данными. Команда предназначена для выполнения на компьютерах с процессором Itanium. Запуск команды на компьютере с архитектурой x86 может завершиться неудачно.

Convert dynamic [noerr]

Преобразование базового диска в динамический. Диск может содержать разделы с данными.

Convert basic [noerr]

Преобразование пустого динамического диска в базовый.

Прочие команды:

Exit. Команда exit служит для завершения программы Diskpart и передачи управления операционной системе.

clean [all]. Удаление всех разделов или томов на диске, имеющем фокус, путем обнуления секторов. По умолчанию переопределяются только сведения о разделах MBR и GPT, а также данные в скрытых секторах на MBR-дисках. Задание параметра all приводит к обнулению всех секторов, в результате чего удаляются все содержащиеся на диске данные.

rem [...] Команда rem не выполняет каких-либо действий, а служит для вставки комментариев в сценарии.

Rescan - Проверка всех шин ввода-вывода и поиск новых дисков, добавленных в компьютер.

Help. Для отображения списка доступных команд служит команда help.

Понятие RAID-массивов

Термин RAID (Redundant Array of Independent/Inexpensive Disks) определяет любую дисковую подсистему, которая объединяет два или более стандартных физических диска в единый логический диск (дисковый массив). Такие дисковые массивы служат для повышения надежности хранения данных и для повышения скорости чтения/записи информации. Они также упрощают сопровождение дисковой подсистемы, так как АС вместо нескольких дисков обслуживает как бы один. Обычно объединение в логический диск осуществляется программно средствами ОС на базе подсистемы ввода-вывода SCSI (для небольших систем на базе SATA). Различают шесть типов (уровней) технологии RAID в зависимости от метода

записи на диски: RAID 0, RAID 1 и т. д.

Рассмотрим особенности различных уровней RAID- массивов и укажем их недостатки и достоинства.

RAID 0 — разделение данных между дисками и чередование блоков. Называется также "Stripe" или "Лента".

Система пишет блоки данных на каждый диск массива подряд (простой стриппинг).

Два или более жестких дисков объединяются в один путем последовательного слияния и суммирования объемов. Т.е. если мы возьмем два диска объемом 500Гб и создадим из них RAID-0, операционной системой это будет восприниматься как один диск объемом в терабайт. При этом скорость чтения/записи у этого массива будет вдвое больше, нежели у одного диска, поскольку, например, если база данных расположена таким образом физически на двух дисках, один пользователь

может производить чтения данных с одного диска, а другой пользователь производить запись на другой диск одновременно. В то время как в случае расположения базы на одном диске, сам жесткий диск задачи чтения/записи разных пользователей будет выполнять последовательно. RAID-0 позволит выполнять чтение/запись параллельно. Как следствие - чем больше дисков в массиве RAID-0, тем быстрее работает сам массив. Зависимость прямо пропорциональная - скорость возрастает в N раз, где N - количество дисков в массиве.

Преимущества: улучшенная производительность и увеличение объема логических томов; разделение данных между дисками позволяет предотвратить ситуации, в которых происходит постоянное обращение к одному диску, в то время как другие диски простаивают.

Недостатки: отсутствие избыточности; поскольку весь массив дисков представляет собой один логический том, то при выходе из строя любого диска из строя выходит весь массив.

RAID 1 — зеркальное отображение/дуплекс. Диски зеркалируются или дублируются. Каждый байт записывается на два идентичных диска. Дублирование добавляет для каждого диска еще и HBA. Работа такой системы уже рассматривалась ранее.

Преимущества: если один диск выходит из строя, другой продолжает работать. Данную концепцию наиболее просто понять и применить. На этом уровне при наличии оптимизированных драйвера и контроллера обычно повышается скорость чтения данных, поскольку можно начать поиск данных на одном диске, в то время как другой диск обрабатывает предыдущий запрос. Однако скорость записи в этом случае замедляется, поскольку данные необходимо записать сразу на два диска. Влияние этой стратегии на производительность зависит от соотношения операций чтения/записи в используемых приложениях.

Недостатки: дороговизна, поскольку для функционирования системы требуется в 2 раз больше дискового пространства, чем это действительно необходимо. Кроме того, необходимо дополнительное место в сервере и дополнительное электропитание.

RAID 5 — разделение данных с чередованием блоков и распределенным контролем четности; разделение блоков данных между всеми дисками. Данные для контроля целостности хранятся на всех дисках. Это хороший компромисс между стоимостью, избыточностью и скоростью. Более безопасный вариант RAID-0. Объем массива рассчитывается по формуле (N - 1) * DiskSize, где N - количество дисков в массиве, а DiskSize - объем каждого диска. Т.е. при создании **RAID-5** из трех дисков по 500Гб, мы получим массив объемом в 1 терабайт. Суть массива

RAID-5 в том, что несколько дисков объединятся в RAID-0, а на последнем диске хранится так называемая "контрольная сумма" - служебная информация, предназначенная для восстановления одного из дисков массива, в случае его смерти. Скорость записи в массиве **RAID-5** несколько ниже, поскольку тратится время на расчет и запись контрольной суммы на отдельный диск, зато скорость чтения такая же, как в RAID-0.

Если один из дисков массива **RAID-5** умирает, резко падает скорость чтения/записи, поскольку все операции сопровождаются дополнительными манипуляциями. Фактически **RAID-5** превращается в RAID-0 и если своевременно не позаботиться восстановлением **RAID-массива** есть существенный риск потерять данные полностью.

С массивом **RAID-5** можно использовать так называемый Spare-диск, т.е. запасной. Во время стабильной работы **RAID-массива** этот диск простаивает и не используется. Однако в случае наступления критической ситуации, восстановление **RAID-массива** начинается автоматически - на запасной диск восстанавливается информация с поврежденного с помощью контрольных сумм, расположенных на отдельном диске.

RAID-5 создается как минимум из трех дисков и спасает от одиночных ошибок. В случае одновременного появления разных ошибок на разных дисках **RAID-5** не спасает.

Преимущества: операции чтения и записи могут осуществляться параллельно, что повышает скорость передачи данных. Этот тип массива высокоэффективен при работе с малыми блоками данных. Предоставляет избыточность с небольшими расходами. Эффективность пятого уровня растет в зависимости от числа дисков, используемых в массиве, поскольку объем данных для контроля целостности обычно занимает один диск, хотя хранятся эти данные на нескольких дисках одновременно. Эффективность дискового массива из трех дисков составляет 66% (один диск используется для контроля четности), а эффективность массива из семи дисков — 86% (так как и в этом случае один диск нужен для контроля четности).

Иногда в массивах пятого уровня используются смонтированные, но бездействующие диски. В случае возникновения неисправности у одного из дисков, входящих в массив, свободный диск может быть автоматически использован для замены поврежденного диска и восстановления данных.

Недостатки: RAID 5 менее производителен, чем RAID 0 или RAID 1 из-за необходимости рассчитывать данные для коррекции ошибок.

Содержание работы

1. Изучить теоретические сведения, порядок работы с утилитой DiskPart.

2. Создать и настроить виртуальную машину в среде Virtual Box для установки Windows Server 2012. Предусмотреть организацию отдельного виртуального контроллера для системного диска и отдельного для дисков хранилища. ***Привод оптических дисков организовать на контроллере SATA для всех вариантов***. Варианты задания представлены в табл. 2.

Таблица 2

Варианты задания для организации виртуальных машин

№ варианта	Кол-во виртуальных носителей хранилища	Тип виртуальных носителей	Формат системного диска	Формат диска хранилища	Тип контроллера хранилища	Тип контроллера системного диска	Массив
1	2	3	4	5	6	7	8
1.	3	*.vdi	Фиксированный	Динамический	SATA	IDE	RAID 0
2.	2	*.vmdk	Фиксированный	Динамический	SCSI	SATA	RAID 1
3.	4	*.vhd	Фиксированный	Динамический	SAS	IDE	RAID 5
4.	2	*.hdd	Фиксированный	Динамический	SATA	IDE	RAID 0
5.	2	*.vdi	Фиксированный	Динамический	SCSI	SATA	RAID 1
6.	3	*.vmdk	Фиксированный	Динамический	SAS	IDE	RAID 5
7.	3	*.vhd	Фиксированный	Динамический	SATA	IDE	RAID 0
8.	2	*.hdd	Фиксированный	Динамический	SCSI	SATA	RAID 1
9.	4	*.vdi	Фиксированный	Динамический	SAS	IDE	RAID 5
10.	4	*.vmdk	Фиксированный	Динамический	SATA	IDE	RAID 0
11.	2	*.vhd	Фиксированный	Динамический	SCSI	SATA	RAID 1

Окончание табл. 2

1	2	3	4	5	6	7	8
12.	3	*.hdd	Фиксированный	Динамический	SAS	IDE	RAID 5
13.	2	*.vdi	Фиксированный	Динамический	SATA	IDE	RAID 0
14.	2	*.vmdk	Фиксированный	Динамический	SCSI	SATA	RAID 1
15.	4	*.vhd	Фиксированный	Динамический	SAS	IDE	RAID 5
16.	2	*.hdd	Фиксированный	Динамический	SATA	IDE	RAID 0
17.	2	*.vdi	Фиксированный	Динамический	SCSI	SATA	RAID 1
18.	3	*.vmdk	Фиксированный	Динамический	SAS	IDE	RAID 5
19.	3	*.vhd	Фиксированный	Динамический	SATA	IDE	RAID 0
20.	2	*.hdd	Фиксированный	Динамический	SCSI	SATA	RAID 1
21.	4	*.vdi	Фиксированный	Динамический	SAS	IDE	RAID 5
22.	3	*.vmdk	Фиксированный	Динамический	SATA	IDE	RAID 0
23.	2	*.vhd	Фиксированный	Динамический	SCSI	SATA	RAID 1
24.	3	*.hdd	Фиксированный	Динамический	SAS	IDE	RAID 5
25.	2	*.vdi	Фиксированный	Динамический	SATA	IDE	RAID 0
26.	2	*.vmdk	Фиксированный	Динамический	SCSI	SATA	RAID 1
27.	3	*.vhd	Фиксированный	Динамический	SAS	IDE	RAID 5
28.	3	*.hdd	Фиксированный	Динамический	SATA	IDE	RAID 0
29.	2	*.vdi	Фиксированный	Динамический	SCSI	SATA	RAID 1
30.	4	*.vmdk	Фиксированный	Динамический	SAS	IDE	RAID 5

3. Выделить отдельный диск под систему и произвести его настройку утилитой DiskPart. **Установка ОС Windows возможна только на диск типа «базовый» !!!**

4. Настроить хранилище утилитой DiskPart по варианту задания (см. табл. 2). Установить и запустить ОС.

5. Рассчитать объем хранилища. Проверить соответствие расчётных данных действительности, убедиться в работоспособности хранилища.

6. Составить отчёт о проделанной работе.

Вопросы для контроля

1. Требования к аппаратным ресурсам средами Windows Server 2012.
2. Понятие производительности системы. Как определяется производительность? От чего зависит?
3. Контроллеры носителей информации виртуальной среды Virtual Box, особенности настроек.
4. Типы виртуальных носителей. Принципы организации.
5. Организация дискового пространства. Особенности носителей MBR.
6. Организация дискового пространства. Особенности носителей GPT.
7. Организация массивов жестких дисков. Технологии, алгоритмы записи данных, расчет количества дисков и объема получаемого пространства.
8. Графический интерфейс управления жесткими дисками Windows Server 2012. Функционал.
9. Утилита DiskPart. Основной функционал.

Лабораторная работа № 2

СЛУЖБА ACTIVE DIRECTORY. УСТАНОВКА, НАСТРОЙКА, АДМИНИСТРИРОВАНИЕ

Цель работы: получить практические навыки настройки контроллера домена, сервера DNS и сервера DHCP. Освоить основы администрирования сети посредством службы Active Directory и сетевых политик безопасности.

Основные сведения

Предлагаемые Microsoft технологии Active Directory прошли длинный путь с момента их появления в версии Windows 2000 Sever. Из одного продукта, называвшегося просто Active Directory (D), в Windows Server 2012 они превратились в пять отдельных технологий. Все они предназначены для обслуживания каталогов и в качестве платформы для интеграции будущих технологий Microsoft. Четыре дополнительных роли службы Active Directory, которые предлагаются в Windows Server 2012, называются так: Active Directoy Lightweight Directory Services - AD LDS (Облегченная служба Active Directory доступа к каталогам), Active Directory Federation Sevices - AD FS (жб. федерации Active Directory), Active Directory Certiicate Services -AD CS (Служба сертификатов Active Directory), Active Directory Rights Management Sevices - AD RMS (Служба правления правами Active Directory). Active Directory Domain Services - AD DS (Доменная служба Active Directory) – традиционная служба обычно применяется на предприятиях в качестве платформы каталогов.

Основные характеристики доменной службы Active Directory

Центральную роль в AD DS играют пять ключевых компонентов. Из-за требований совместимости новых служб каталогов со стандартами Интернета в существующие реализации были внесены соответствующие изменения и уделено больше внимания перечисленным ниже областям.

- **Совместимость с TCP/IP.** В отличие от ряда специализированных протоколов вроде IPX/SPX и NetBEUI, протокол TCP/IP с самого начала создавался межплатформенным. Последующее принятие TCP/IP в качестве Интернет-стандарта для обмена данными сделало его одним из лидеров в мире протоколов и, по сути, превратило в обязательный протокол для операционных систем уровня предприятия. В AD DS и Windows

Server 2012 стек протоколов TCP/IP используется в качестве основного метода для обмена данными.

• **Поддержка протокола LDAP.** Протокол LDAP (Lightweight Directory Access Protocol — облегченный протокол доступа к каталогам) был разработан в качестве стандартного Интернет-протокола для доступа к каталогам. Он применяется для обновления и запросов данных, хранящихся в каталогах. Служба AD DS непосредственно поддерживает LDAP.

• **Поддержка системы доменных имен.** Система доменных имен (Domain Name System — DNS) была создана для преобразования упрощенных имей, понятных людям (таких как www. cco. com), в IP-адреса, понятные компьютерам (вроде 12.222.165.154). В AD DS она поддерживается и даже требуется для нормальной работы.

• **Поддержка безопасности.** Поддержка безопасности в соответствии со стандартами Интернета чрезвычайно важна для бесперебойного функционирования среды, к которой подключены миллионы компьютеров по всему миру. Отсутствие надежных средств защиты привлекает хакеров, поэтому в Windows Server 2012 и AD DS средства безопасности были значительно расширены. Так, в Windows Server 2012 и AD DS была встроена непосредственная поддержка IPSec, Kerberos, центров сертификации и шифрования с помощью протокола защищенных сокетов (Secure Sockets Layer — SSL).

• **Легкость администрирования.** При реализации мощных служб каталогов удобству администрирования и конфигурирования среды часто не уделяется должного внимания. А зря: этот аспект очень сильно влияет на общую стоимость эксплуатации. AD DS и Windows Server 2012 специально спроектированы так, чтобы ими было удобно пользоваться, и чтобы на освоение новой среды тратилось как можно меньше усилий. Для улучшения администрирования AD DS в Windows Server 2012 добавлены компоненты Active Directory Administration Center (Центр администрирования Active Directory), Active Directory Web Services (Веб-служба Active Directory) и модуль для администрирования Active Directory из оболочки Windows PowerShell.

Структура AD DS

Логическая структура AD DS позволяет выбрать ее размер и для небольших офисов, и для крупных международных организаций. Встроенная возможность детализации обязанностей, связанных с администрированием, позволяет делегировать управление группам пользовате-

лей или отдельным пользователям. Предоставление прав на администрирование по принципу "все или ничего" осталось в прошлом. AD DS в основном следует модели каталогов X.500, но обладает и рядом собственных характеристик. Многие уже привыкли к лесам и деревьям AD DS, а некоторые ограничения, которые имелись в предыдущих версиях AD DS, теперь устранены. Чтобы понять AD DS, сначала нужно разобраться в ее основных структурных компонентах.

Домен AD DS

Домен AD DS, традиционно изображаемый в виде треугольника (рис. 1), является главной логической границей AD DS.

Рис. 1. Обозначение домена

В некотором смысле структура домена AD DS во многом схожа с более ранней структурой доменов Windows NT 4.0, которую он заменил. Информация о пользователях и компьютерах хранится и обрабатывается внутри домена. Однако появилось несколько серьезных изменений в структуре домена и в способе его взаимодействия с другими доменами в структуре AD DS.

Домены в AD DS разграничивают административную безопасность для объектов и содержат собственные политики безопасности. Важно помнить, что домены представляют собой логическую организацию объектов и могут охватывать несколько физических местоположений. Значит, уже не нужно создавать множество доменов для различных удаленных офисов или вычислительных центров, поскольку вопросы репликации и безопасности теперь гораздо удобнее решать с помощью сайтов AD DS или контроллеров RODC.

Деревья доменов AD DS

Дерево AD DS состоит из нескольких доменов, соединенных двунаправленными транзитивными отношениями доверия. Каждый домен в дереве AD DS использует общую схему и глобальный каталог. Корневым доменом дерева ADDS является companyabc.com, а asia.companyabc.com и europe.companyabc. com — его поддомены (см. рис. 2).

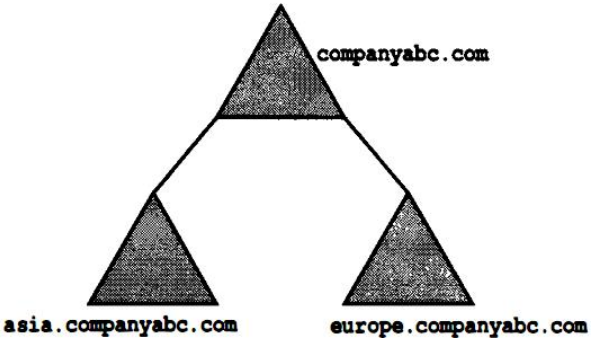

Рис. 2. Дерево ADDS с поддоменами

Транзитивное отношение доверия устанавливается автоматически. Оно означает, что если домен asia доверяет корневому домену companyabc, и домен europe также доверяет домену companyabc, то домен asia доверяет и домену europe. Доверительные отношения пронизывают всю доменную структуру.

Транзитивность отношений доверия в среде AD DS не означает, что правами доступа могут пользоваться все пользователи или даже администраторы других доменов. Доверительные отношения лишь обеспечивают путь от одного домена к другому. По умолчанию никакие права доступа от одного транзитивного домена к другому не передаются. Чтобы пользователи или администраторы другого домена могли получать доступ к ресурсам данного домена, его администратор должен предоставить им соответствующие права.

Все входящие в состав дерева домены используют общее пространство имен (в данном примере — companyabc. com), но содержат механизмы защиты для разграничения доступа из других доменов. То есть администратор домена europe может иметь относительный контроль над всем его доменом, а пользователи из домена asia или companyabc могут не располагать полномочиями на доступ к его ресурсам. Однако при желании администратор europe может разрешить каким-то группам пользователей из других доменов обращаться к ресурсам его домена. Права на администрирование могут назначаться очень избирательно.

Кстати, возможность создания поддоменов в лесе, как на рис. 2, не означает, что это обязательно имеет смысл. Многие среды замечательно обслуживаются одним доменом для всех их ресурсов, разбросанных по миру. А после создания поддоменов становится не очень легко перемещать ресурсы.

Леса в AD DS

Лесами (forest) в AD DS называются группы связанных между собой деревьев доменов. Неявные отношения доверия объединяют корни всех деревьев в один общий лес.

Связями, объединяющими все домены и деревья доменов в общий лес, служит наличие общей схемы и общего глобального каталога. Хотя доменам и деревья доменов в этом лесу вовсе не обязательно использовать общее пространство имен. Например, домены microsoft. internal и msnbc. internal теоретически могут являться частями одного и того же леса, но при этом иметь собственные раздельные пространства имен.

Леса служат основной границей организационной безопасности в AD DS, и потому предполагают наличие некоторой степени доверия к администраторам всех входящих в их состав доменов.

Режимы аутентификации в AD DS

В Windows NT 4.0 для аутентификации применялась подсистема под названием NTLM (NT LAN Manager — диспетчер локальной сети NT). В ней зашифрованный пароль пересылался по сети в виде хеша. Ее недостатком было то, что любой желающий мог отслеживать в сети передаваемые хеши, собирать их и затем расшифровывать с помощью сторонних средств взлома паролей по словарю или "грубой силой".

Во всех версиях Windows Server после Windows 2000 стала применяться подсистема аутентификации Kerberos. Kerberos не пересылает информацию пароля по сети и поэтому гораздо безопаснее NTLM.

Обзор функциональных уровней в Windows Server 2012 AD DS

В Windows 2000 Server и Windows Server 2003 поддерживались собственные функциональные уровни для обеспечения обратной совместимости с доменами предыдущих версий. Аналогично Windows Server 2012 содержит функциональные уровни для поддержки совместимости.

По умолчанию при выполнении свежей установки Active Directory на контроллерах домена Windows Server 2012 автоматически создается домен Windows Server 2012 и функциональные уровни леса. Но при установке контроллеров домена Windows Server 2012 в существующем устаревшем домене можно выбрать функциональный уровень, с которого начнет работать лес Если лес Active Directory уже существует, его функциональный уровень можно поднять до Windows Server 2012 следующим образом.

• Проверьте, что все контроллеры доменов в лесе обновлены до Windows Server 2012 или заменены новыми контроллерами Windows Server 2012.

• В диспетчере серверов на контроллере домена выберите в меню Tools (Сервис) пункт Active Directory Domains and Trusts (Active Directory — домены и доверие).

• В левой панели щелкните правой кнопкой мыши на имени нужного домена и выберите в контекстном меню пункт Raise Domain Functional Level (Повысить функциональный уровень домена).

• В окне Raise Domain Functional Level выберите вариант Windows Server 2012 и щелкните на кнопке Raise (Повысить).

• Два раза щелкните на кнопках OK, чтобы завершить выполнение задачи.

• Повторите шаги 1-5 для всех остальных доменов в лесе.

• Выполните такие же шаги для корневого дерева леса, но на этот раз выберите вариант Raise Forest Functional Level (Повысить функциональный уровень леса) и следуйте выводимым подсказкам.

После повышения уровня всех доменов и леса до Windows Server 2012 в лесе можно будет использовать новейшие функциональные средства AD DS. Важно помнить, что до выполнения этой процедуры в среде со смешанными режимами Windows Server 2012 работает в более низком режиме совместимости.

Обзор компонентов AD DS

Основные компоненты AD DS изначально разрабатывались с целью легкости их настройки и защиты. AD DS и все ее составляющие физически размещаются в одном файле базы данных, но содержат самые разнообразные объекты и их атрибуты. Многие из описываемых характеристик наверняка известны тем, кто знаком с другими службами каталогов, но среди них есть и новинки.

Связь AD DS с моделью X.500

AD DS в основном следует информационной модели службы каталогов X.500, которая определяет службу каталогов через распределенный подход, определенный информационным деревом каталога (Directory Information Tree — DIT). Это дерево логически разбивает структуру службы каталогов в уже знакомый формат: *имя_сервера.имя_поддомена.имя_домена.com*

В модели X.500 информация каталога хранится в иерархической структуре, получившей название агентов системы каталогов (Directory

System Agent — DSA). Технология AD DS основана на многих базовых принципах определения X.500, но сама AD DS не совместима с реализациями X.500, поскольку протокол X.500 основан на модели OSI, которая неэффективно работает с протоколом TCP/IP, используемым AD DS.

Концепция схемы AD DS

Схемой в AD DS называется набор определений для всех типов имеющихся в каталоге объектов и связанных с ними атрибутов. Именно схема задает способ хранения и представления в AD DS данных обо всех пользователях, компьютерах и других объектах, чтобы они имели стандартный вид по всей структуре AD DS. Она защищается с помощью списков управления разграничением доступа (Discretionary Access Control List - DACL) и отвечает за предоставление возможных атрибутов для каждого объекта в AD DS. По сути, схема представляет собой базовое определение самого каталога и является основой функционирования среды домена. При делегировании прав на управление схемой избранной группе администраторов следует соблюдать осторожность, поскольку вносимые в схему изменения влияют на всю среду AD DS.

Объекты схемы

Сохраняемые внутри структуры AD DS элементы, вроде пользователей, принтеров, компьютеров и сайтов, в рамках схемы называются объектами. У каждого такого объекта имеется свой список атрибутов, которые определяют его характеристики и могут применяться для его поиска. Например, объект пользователя для работника по имени Иван Петров будет иметь атрибут FirstName (Имя) со значением "Иван" и атрибут LastName (Фамилия) со значением "Петров". Помимо этих, могут назначаться и другие атрибуты: название подразделения, адрес электронной почты и многое другое. Пользователи, которые выполняют поиск информации в AD DS, смогут строить на основе этой информации свои запросы и находить, например, всех пользователей, которые работают в отделе сбыта.

Расширение схемы

Одним из главных преимуществ структуры AD DS является возможность напрямую изменять и расширять схему, включая в нее произвольные атрибуты. Обычно расширение набора атрибутов происходит во время установки системы Microsoft Exchange Server, когда схема значительно увеличивается в размере. При обновлении с Windows Server 2003

или Windows Server 2008 AD до Windows Server 2012 AD DS тоже происходит расширение схемы, и в нее добавляются атрибуты, характерные для Windows Server 2012. Многие сторонние продукты также выполняют свои расширения схемы, которые позволяют отображать различные типы информации из каталога. Учтите, что расширения схемы следует выполнять только в случаях абсолютной необходимости, поскольку неаккуратное расширение может внести хаос в среду AD DS.

Внесение изменений в схему с помощью утилиты ADSI

Для просмотра всех деталей схемы AD DS существует интересный способ - использование утилиты ADSIEdit (AD DS Service Interfaces - интерфейсы службы AD DS). Эта утилита разработана для упрощения доступа к AD DS, однако она позволяет просматривать и любые другие совместимые внешние каталоги LDAP. Она позволяет просматривать, удалять и изменять атрибуты схемы. Соблюдайте предельную осторожность при внесении изменений в схему, поскольку проблемы в схеме сложно устранить.

Облегченный протокол доступа к каталогам

В основе протокола службы каталогов (Directory Service Protocol), который используется в AD DS, лежит совместимый со стандартом Интернета облегченный протокол доступа к каталогам (Lightweight Directory Access Protocol — LDAP), определенный в документе RFC-3377.

Протокол LDAP позволяет выполнять запросы и изменения в AD DS. Объекты в совместимых с LDAP каталогах, должны уникально идентифицироваться их именующими путями. Эти именующие пути могут принимать две формы: отличительные и относительные отличительные имена.

Пример настройки контроллера домена

Задание: настроить сервер в режим работы контроллера домена. Установить и настроить службы Active Directory (ADDS), DNS, DHCP. Для группы GAdm назначить следующие права: включать в домен ПК сети, управление удалёнными рабочим столом.

1. Сначала необходимо установить соответствующие роли сервера (см. рис. 3). Управление ролями вызывается через диспетчера сервера, запускающийся автоматически при старте ОС.

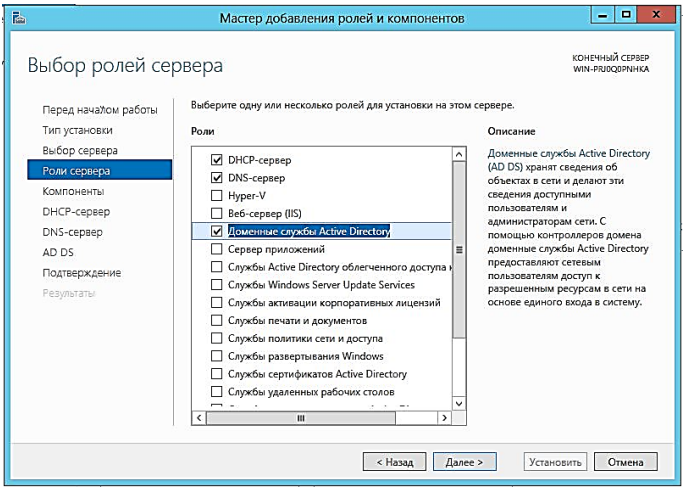

Рис. 3. Мастер добавления ролей

После успешной установки ролей сервер необходимо перезагрузить.

2. Каждая служба после установки нуждается в настройке или проверке функционирования. Обратиться к настройкам служб можно, например, через систему уведомлений, нажав соответствующую надпись (см. рис. 4).

3. После того, как настроены роли DHCP и DNS, необходимо инициализировать службу ADDS (см. рис. 5 слева-направо, сверху-вниз). При задании пароля следует учитывать политику паролей контроллера домена: длина – не менее восьми символов, должна быть хотя бы одна большая буква, а остальные могут быть в любом регистре, хотя бы одна цифра.

Пути к базе данных, файлам журнала и системному каталогу рекомендуется оставить без изменений.

После проверки параметров и настроек служб и компонентов контроллера домена следует произвести их установку (нажать кнопку «Установить» в разделе «Установка»).

Управление контроллером домена осуществляется через утилиты консоли MMC, системные ярлыки на которые автоматически создаются в главном меню. Вынести ярлыки в другие места возможно через контекстное меню, открыв расположение системных ярлыков.

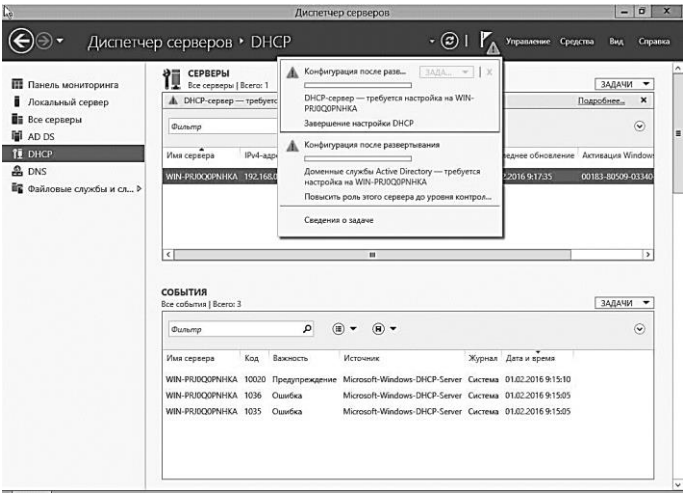

Рис. 4. Настройка ролей

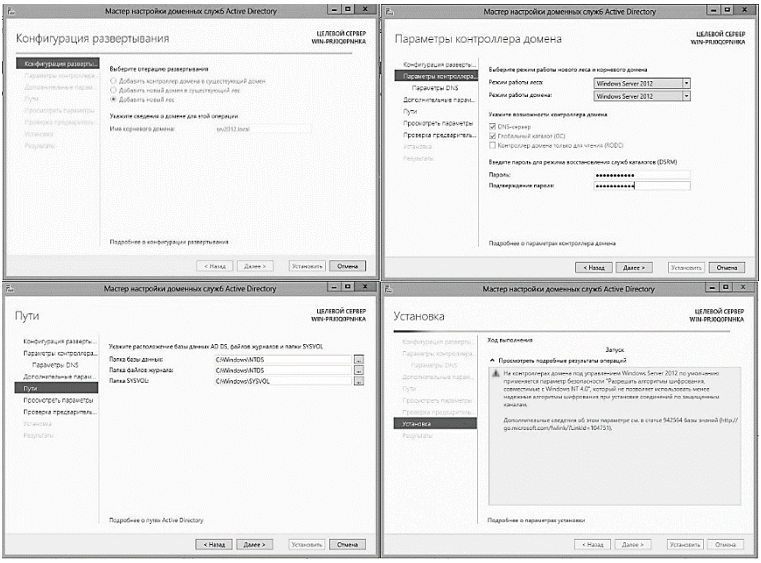

Рис. 5. Инициализация службы ADDS

4. Чтобы изменять состав групп и пользователей домена, необходимо использовать утилиту Пользователи и группы Active Directory. Согласно задания, создаются 3 папки в структуре леса с соответствующими именами, 3 учетные записи пользователей, располагающихся в

этих папках, назначается членство пользователей в группах. По умолчанию все пользователи и группы находятся в папке Users. Их можно переносить обычным перетаскиванием или через контекстное меню. Все параметры учетной записи или группы изменяются в свойствах (рис. 6).

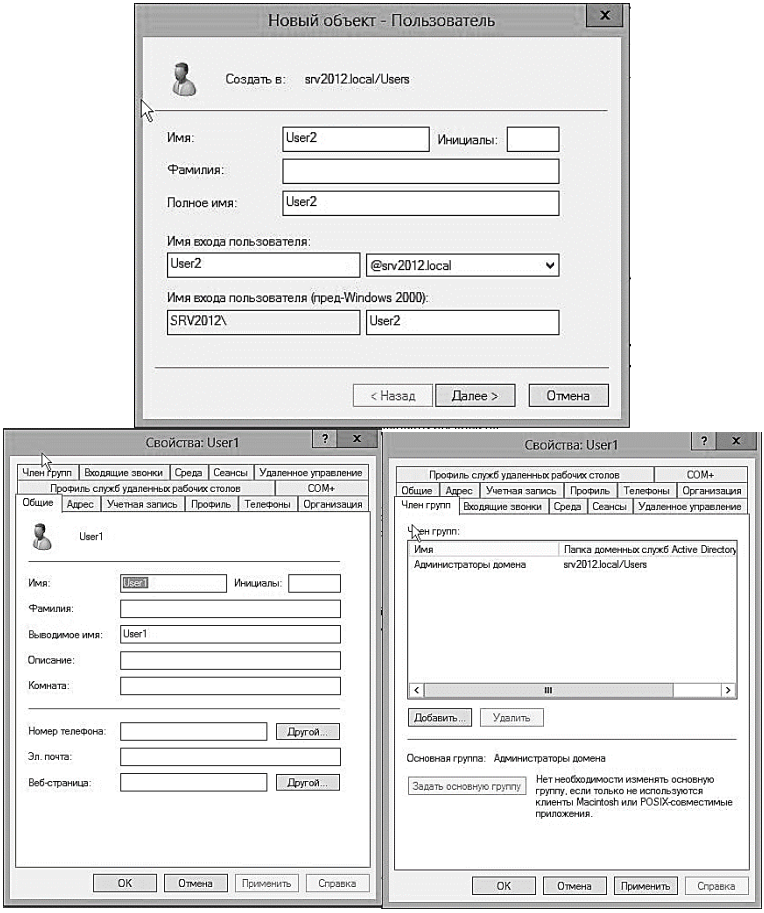

Рис. 6. Управление учетными записями

Чтобы изменить группу принадлежности пользователя, необходимо добавить в список членства групп предпочтительную группу, назначить

ее основной, удалить все ненужные группы. Таким образом пользователь унаследует все права от политик группы, оставленной в списке членства групп. Если в списке содержится несколько групп, то права пользователю назначаются в порядке их иерархии от высокоприоритетных к низкоприоритетным.

5. Создание нестандартных политик безопасности возможно посредством инструмента – Управление групповой политикой (см. рис. 7), раздел «Объекты групповой политики». Создание групповой политики осуществляется несколькими способами, например, через контекстное меню папки «Объекты групповой политики». Далее, чтобы делегировать права группе от созданной политики, необходимо выбрать инструмент «Изменить» в контекстном меню самой политики. Далее, как показано на рис. 8, выставить права группам и пользователям, подчиняющимся данной политике. Так же назначить права созданной или любой другой группе возможно, изменив политику по умолчанию - Default Domain Controllers Policy. Данная политика является корневой для всего контроллера домена и имеет высший приоритет. Если какое-то правило в созданной политике не указано, оно делегируется из вышестоящей.

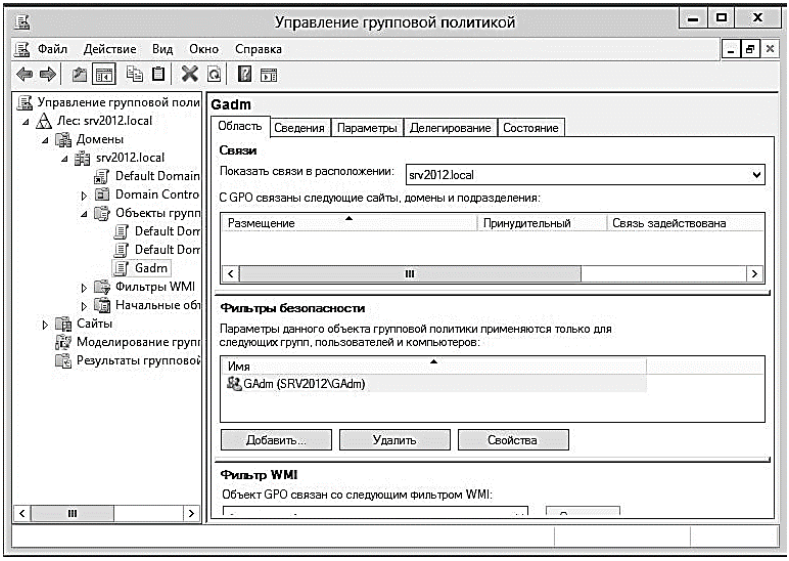

Рис. 7. Управление политиками домена

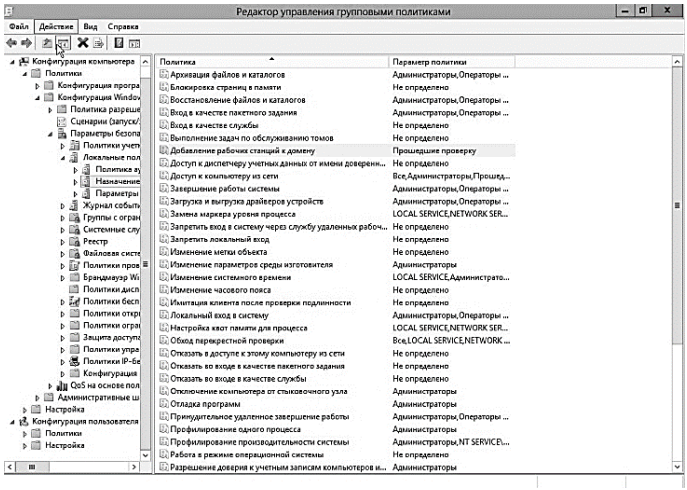

Рис. 8. Назначение прав

Содержание работы

1. Изучить теоретические сведения. Освоить способы создания групповых политик безопасности в ADDS.

2. Настроить сервер в режим работы контроллера домена: установить и настроить службы Active Directory (ADDS), DNS, DHCP. Варианты задания представлены в табл. 3. Для группы NAdmin назначить следующие права: включать в домен ПК сети, управление удалёнными рабочим столом.

Таблица 3

Варианты заданий для организации доменных служб

№ варианта	Имя контроллера домена	Имя зоны DNS	Создаваемые папки	Пользователи	Роли пользователей
1	2	3	4	5	6
1.	Dom1.it4	Dns1	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin1
2.	Dom2.it4	Dns2	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin2

Продолжение табл. 3

1	2	3	4	5	6
3.	Dom3.it4	Dns3	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin3
4.	Dom4.it4	Dns4	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin4
5.	Dom5.it4	Dns5	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin5
6.	Dom6.it4	Dns6	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin6
7.	Dom7.it4	Dns7	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin7
8.	Dom8.it4	Dns8	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin8
9.	Dom9.it4	Dns9	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin9
10.	Dom10.it4	Dns10	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin10
11.	Dom11.it4	Dns11	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin11
12.	Dom12.it4	Dns12	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin12
13.	Dom13.it4	Dns13	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin13
14.	Dom14.it4	Dns14	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin14
15.	Dom15.it4	Dns15	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin15
16.	Dom16.it4	Dns16	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin16
17.	Dom17.it4	Dns17	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin17

Окончание табл. 3

1	2	3	4	5	6
18.	Dom18.it4	Dns18	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin18
19.	Dom19.it4	Dns19	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin19
20.	Dom20.it4	Dns20	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin20
21.	Dom21.it4	Dns21	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin21
22.	Dom22.it4	Dns22	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin22
23.	Dom23.it4	Dns23	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin23
24.	Dom24.it4	Dns24	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin24
25.	Dom25.it4	Dns25	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin25
26.	Dom26.it4	Dns26	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin26
27.	Dom27.it4	Dns27	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin27
28.	Dom28.it4	Dns28	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin28
29.	Dom29.it4	Dns29	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin29
30.	Dom30.it4	Dns30	Group1	User1	Domain Admin
			Group2	User2	Domain User
			Group3	User3	NAdmin30

3. Установить вторую гостевую ОС со средой Windows. Включить ее в созданный домен, используя учетную запись пользователя группы NAdmin.

4. Проверить назначение прав и работу каждой из учетных записей во второй гостевой ОС, например, посредством изменения даты и времени.

5. Проверить работу DHCP-сервера. Проверить записи DNS-сервера. Протестировать работу добавленных записей.

6. Составить отчет о проделанной работе.

Вопросы для контроля

1. Виды служб каталогов, назначение.
2. Основные характеристики доменной службы Active Directory.
3. Структура AD DS.
4. Домен AD DS.
5. Деревья доменов AD DS. Понятия, свойства.
6. Леса в AD DS.
7. Режимы аутентификации в AD DS.
8. Обзор функциональных уровней в Windows Server 2012 AD DS.
9. Обзор компонентов AD DS.
10. Связь AD DS с моделью X.500.
11. Концепция схемы AD DS.
12. Объекты схемы AD DS.
13. Расширение схемы AD DS.
14. Внесение изменений в схему с помощью утилиты ADSI.
15. Облегченный протокол доступа к каталогам AD DS.
16. Способы создания политик безопасности, особенности, наследование и делегирование прав.
17. DNS служба, принцип и особенности работы.
18. DHCP сервер, особенности настройки, принцип работы.
19. Этапы включения ПК в домен.
20. Репликация служб каталогов.

Лабораторная работа № 3

АДМИНИСТРИРОВАНИЕ СЕТЕВЫХ ПОТОКОВ ДАННЫХ

Цель работы: изучить принципы и методы администрировании информационных потоков в информационных сетях посредством файервола, установленного на маршрутизаторе.

Основные сведения

Основы работы в сети и анализ сети

Приступая к обеспечению безопасности компьютера, нужно иметь представление о том, как работают сетевые службы, какие службы действуют в настоящее время, какие порты открыты и т. д.

Прежде всего рассмотрим табл. 4, в которой в обобщенном виде представлены важнейшие сокращения.

Таблица 4

Важнейшие сокращения сетевых терминов

Сокращение	Значение
DNS	Служба доменных имен
HTTP	Протокол передачи гипертекста
ICMP	Протокол управления сообщениями в Интернете
IP	Интернет-протокол
NFS	Сетевая файловая система
TCP	Протокол управления передачей
UDP	Протокол пользовательских датаграмм

Кроме самих данных, в IP-пакетах содержатся (в том числе) еще четыре важных фрагмента информации: IP-адрес отправителя, порт отправителя, адрес назначения и порт получателя. Благодаря этим данным становится известно, откуда приходит пакет и куда он должен быть направлен.

IP-адреса и порты. Вы уже понимаете, зачем нужен IP-адрес. IP-порты применяются для идентификации различных служб. Например, для запроса веб-документа обычно используется порт 80. Номера портов — это 16-битные числа. Порты вплоть до 1024 считаются привилегированными и зарезервированы для серверных служб (например, для HTTP-сервера). Остальные порты могут использоваться и клиентами, но и среди них есть несколько номеров, которые не должны применяться клиентом, так как в свою очередь зарезервированы для выполнения определенных целей.

Для многих IP-номеров портов заданы псевдонимы. В табл. 5 перечислены важнейшие номера портов, а также имена, под которыми они обычно используются (если такие имена есть), и краткое объяснение.

Таблица 5

Важнейшие IP-порты

Название	Порт	Функция
Icmp	8	Протокол управления сообщениями
ftp	20,21	FTP
ssh	22	SSH
telnet	23	Telnet
smtp	25	Электронная почта
domain	53	DNS
Bootps и bootpc	67, 68	DHCP
http	80	Сеть
kerberos	88	Kerberos
pop3	110	Электронная почта
portmap	111	Portmap (для NFS)
ntp	123	Время (сетевой протокол синхронизации времени)
netbios-ns	137	Служба имен Microsoft/NetBIOS
netbios-dgm	138	Служба датаграмм Microsoft/NetBIOS
netbios-ssn	139	Служба доступа к файлам Microsoft (SMB, Samba)
imap	143	Электронная почта
ldap	389	LDAP
	427, 548	Файловый протокол Apple (AFP)
https	443	Сеть (зашифрованный)
microsoft-ds	445	Файловая система CIFS (SMB, Samba)
printer	515	Печать с использованием LPD/LPR
ipp	631	Печать с использованием IPP/CUPS
rmi	1099	Удаленный вызов методов (Java)
	1433	Microsoft SQL Server
pptp	1723	PPTP/VPN
nfs	2049	NFS
	3128	Squid (сетевые прокси)
mysql	3306	Сервер базы данных MySQL
	5999-6003	X-дисплей
	9100	Сетевой принтер HP-JetDirect

Настройка маршрутизатора в режиме форвардинга

Принципы построения маршрутов как в Windows, так и в Linux одинаковы. Отличается только синтаксис команд. Важно учесть такую особенность Linux, как чувствительность к регистру ввода команд, ввод

производится только в нижнем регистре, за исключением отдельных ключей (нужно смотреть справку по команде в Linux).

В Linux таблица маршрутизации вызывается командой route (см. рис. 9).

Если при добавлении маршрута не указывается конкретный интерфейс, с которым будет взаимосвязан маршрут, то этот маршрут открывается для всех интерфейсов, имеющихся на данном ПК.

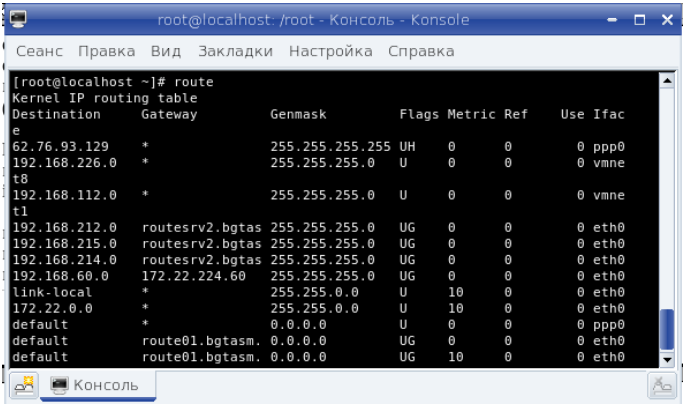

Рис. 9. Пример таблицы маршрутизации в Linux

Рекомендуется сначала просмотреть настройки сетевых интерфейсов на ПК. Таблица настройки интерфейсов вызывается командой ifconfig.

На экран выводится полная таблица настроек всех сетевых интерфейсов, которые подключены к данной машине (см. рис. 10). eth* - физические интерфейсы, ppp - это виртуальный интерфейс для VPN сети, vmnet* - интерфейс виртуальной машины, lo - локальный интерфейс, служащий для серверной связи между собой приложений (для организации системы клиент-сервер локально). * - обозначается порядковый номер интерфейса. Для интерфейсов в Linux нумерация начинается с 0.

Если необходимо просмотреть настройки какого-то конкретного сетевого интерфейса, тогда команда ifconfig выполняется с параметром (название сетевого интерфейса в системе).

ifconfig eth0

При выполнении команды с таким параметром на экран выведется таблица настроек для интерфейса eth0 (см. рис. 11).

В Linux справка по командам вызывается следующим образом: пишется команда, причем, если не знать точного названия команды, но

помнить начало, то с помощью клавиши Tab консоль сама находит все варианты набранного фрагмента команды, дописываем её до конца, далее ставиться двойной минус и пишется команда help, например, команда route:

route –help

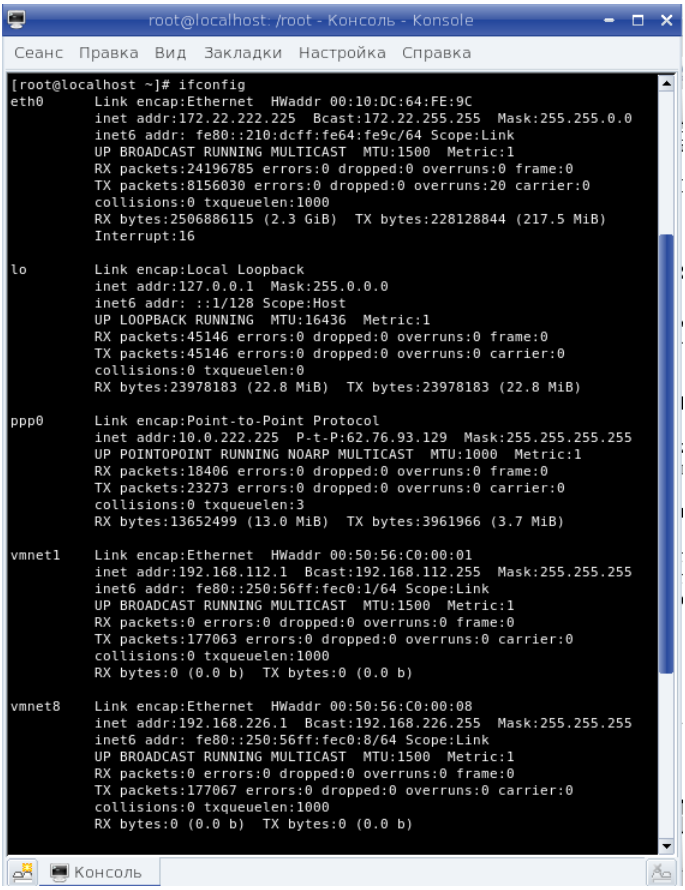

Рис. 10. Таблица настроек сетевых интерфейсов

Добавление маршрутов в Linux осуществляется командой route с ключом add. Стоит обратить внимание на регистр вводимых символов, Linux чувствителен к регистру. Следом указывается ключ, определяющий тип маршрута. Если добавляемый маршрут делается статическим,

то указывается ключ -net. Таким образом, команда с ключами route add -net означает: добавить статический маршрут. В отличие от Windows статические маршруты Linux не сохраняются при перезагрузке машины, но сохраняются при перезагрузке сетевых интерфейсов и настроек. Обычные маршруты, которые добавляются без каких-либо ключей, удаляются при перезагрузке сетевых интерфейсов.

Команда для добавления маршрута выглядит следующим образом:

route add -net 192.x.x.x netmask 255.255.x.x gw x.x.x.x eth*

route add -net добавляет статический маршрут на подсеть с сетевым идентификатором 192.x.x.x, netmask указывает, с какой маской используется подсеть, gw описывает адрес шлюза (x.x.x.x), через который осуществляется доступ к данной подсети. Далее указывается через какой интерфейс будет идти обращение в эту подсетку — eth*.

Также можно указывать количество бит маски через косую черту. Если добавляется временный маршрут, то команда выглядит следующим образом:

route add 192.x.x.x/y gw x.x.x.x eth*

Если шлюз в данной машине один, тогда имеет место следующая запись команды:

route add -net 192.x.x.x/y gw default eth*

Default означает, что будет использоваться шлюз по умолчанию.

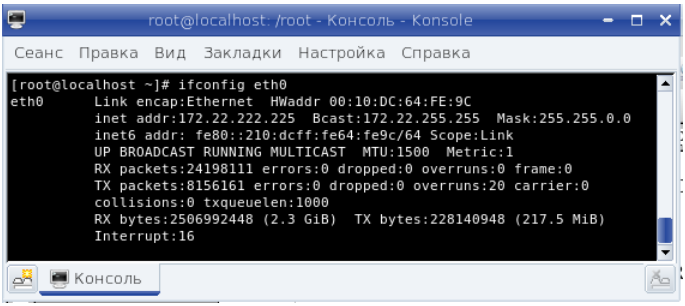

Рис. 11. Параметры для интерфейса eth0

Рассмотрим настройку маршрутизатора на примере Linux Rosa. В *nix-подобных системах все настройки и информация об оборудовании хранятся в текстовых файлах. Все устройсва в Linux отображаются в папке /dev/. Настройки - /etc/.

Настройки сетевых интерфейсов находятся в папке /etc/sysconfig/network-scripts/ifcfg-*. Вместо звездочки указывается системное имя интерфейса (eth0, eth1 и т.д.). Сколько установлено физических интерфейсов, столько будет файлов конфигурации.

Чтобы настроить маршрутизатор, необходимо один из сетевых интерфейсов сделать шлюзом для остальных сетевых интерфейсов, установленных в данном системном блоке. Для этого используется функция IP форвардинга — перенаправление пакетов IP. За запуск сети отвечает скрипт networking в папке /etc/sysconfig/. В нем нужно указать опцию включения форвардинга при запуске сетевых интерфейсов и настроить их соответствующим образом. При наборе пути файла и папки в консоли, а также названий стандартных или установленных служб, допускается использовать автозаполнение клавишей Tab. Например, если необходимо указать путь /etc/sysconfig/, то можно набрать в консоли /etc/sysc и нажать клавишу автозаполнения, получим сразу введенный путь к папке - /etc/sysconfig/.

Часто для вспомогательных действий используют файловые менеджеры. В Linux самый распространенный – Midnight Commander (вызывается командой в консоли mc). В этой оболочке существует быстрый фильтр поиска файлов и папок – сочетание клавиш ***Ctrl+x*** потом ***s*** – при этом появится внизу активного окна строка фильтра, при наборе имени курсор автоматически будет переходит сверху вниз (только так!!!) к первой в списке папке с максимально совпадающим именем с набранным. Для копирования пути к папке в mc существует сочетание ***Escape*** затем ***a***, путь скопируется и вставится в командную строку mc, путь к файлу – ***Escape*** потом ***Enter***. То есть чтобы указать полный путь к файлу, необходимо поставить курсор на файл и нажать ***Escape a, Escape Enter***. Остальные команды схожи с FAR.

Пример настройки маршрутизатора в режим форвардинга

По умолчанию в системах Linux сетевые интерфейсы называются eth*, где * - номер интерфейса. Их можно переименовать по своему усмотрению. Настройки сетевых интерфейсов хранятся в /etc/sysconfig/network-scripts/, их имена – ifcfg-*, где * - имя интерфейса.

Порядок настройки маршрутизатора:

1. войти в папку /etc/sysconfig/network-scripts/;
2. определить шлюзовой интерфейс (обычно eth0), настроить его должным образом:
   ifcfg-*:
   BOOTPROTO=static

IPADDR=x.x.x.x
NETMASK=y.y.y.y
MII_NOT_SUPPORD=yes
ONBOOT=yes

3. настроить сетевой интерфейс для подсети:
   ifcfg-*:
   BOOTPROTO=static
   IPADDR=x1.x1.x1.x1
   NETMASK=y1.y1.y1.y1
   MII_NOT_SUPPORD=yes
   ONBOOT=yes
4. включить сетевые шлюзовые параметры, добавив в скрипт /etc/sysconfig/network строку:
   GATEWAYDEV=<имя шлюзового интерфейса>
5. разрешить IP-форвардинг, настроив скрипт /etc/sysctl.d/<имя>.conf. Найти строчку net.ipv4.ip_forward, изменить ее на net.ipv4.ip_forward = 1. Если строка отсутствует, то добавить ее в файл. Сохранить файл;
6. перезапустить службу network, в консоли команда:
   service network restart;
7. просмотреть процесс форвардинга:
   cat /proc/sys/net/ipv4/ip_forward (должен содержать «1»);
8. остановить службы shorewall и iptables.
9. проверить работоспособность маршрутизатора посредством команды ping. По умолчанию при выключенном файерволе или при всех разрешениях эхо-пакеты проходят между всеми интерфейсами сет;
10. перезапустить маршрутизатор (reboot).

Настройка Shorewall

Настройки файервола содержатся в папке /etc/shorewall/ и состоят из нескольких важных частей: зоны (zones), интерфейсы (interfaces), глобальные (высокоуровневые) правила (policy) и правила пользователя (rules). Отделять один параметр от другого следует табуляцией.

Порядок настройки:

1. zones – в этом файле описываются логические зоны файервола. Их может быть больше, чем физических интерфейсов. Имена зон допускается менять на усмотрение пользователя **(они не должны совпадать с именами интерфейсов!!!)**. Каждой зоне присваивают её тип, например,

firewall или ipv4. Строка конфигурации логической зоны содержит 4 параметра: имя зоны, тип, общие опции, опции входа, опции выхода. Опции допускается не указывать. Например:

fw firewall
net1 ipv4

2. interfaces содержит соответствие логических зон физическим сетевым интерфейсам. Каждому сетевому интерфейсу должна быть назначена только одна логическая зона. Строка описания интерфейсов содержит 3 параметра: зона, имя интерфейса, опция. Имя интерфейса должно соответствовать реальному (по умолчанию eth0, eth1 и т.д.). Опция detect включает весь трафик на интерфейсе, включая широковещательный.

3. policy содержит глобальные правила использования зон. Обычно в них запрещают весь трафик. Строка описания правил содержит 6 параметров, важны из которых 3: “откуда” (sources), “куда” (dest) и правило (policy). В опциях “откуда” и “куда” указываются зоны. Если необходимо указать все зоны сразу, то их описывают параметром all. Обычно для зон используют 3 правила: ACCEPT – разрешить, DROP – запретить и REJECT – запретить с отправкой ответа пользователю. Обычно по умолчанию запрещаются весь трафик:

all all REJECT.

4. В файле rules содержаться правила движения трафика, заданные пользователем. Формат строки основных параметров следующий:

Action source dest proto ports

Action – политика (ACCEPT, DROP, REJECT). Также возможно указывать имена макросов (формат имени файла макроса: macro.USER, где USER – имя макроса) с указанием политики, например, USER(ACCEPT).

Source – источник информационного потока.

Dest – приемник информационного потока.

Как в source так и в dest обязательно указывается зона. Также возможно определить отдельные адреса в правилах, или подсети, к которым они относятся. Форматы параметров следующие: <имя зоны>, <имя зоны>:<IP>, <имя зоны>:<префикс сети>. Знак <> носит формализующий характер и не указывается в файле rules.

Proto – имя сетевого протокола, например, tcp, udp, icmp.

Ports – указывает порты соответствующего протокола.

Пример:

Даны 3 зоны fw, n1 и n2, где n1, n2 соответствуют физическим интерфейсам с именами eth0 и eth1 соответственно. Fw – firewall.

Необходимо разрешить прохождение трафика по порту 5555 протокола tcp в обе стороны, а по порту 352 протокола udp – доступ к маршрутизатору со стороны интерфейса eth1.

В файле rules должны содержаться следующие строки:

ACCEPT	n1	n2	tcp	5555	-
ACCEPT	n2	n1	tcp	5555	-
ACCEPT	n2	fw	udp	352	-

Макросы хранятся в папке /usr/share/shorewall/. Формат имени файла macro.*, где * - имя макроса, которое применяется для макроподстановок в правилах файервола.

Содержание работы

1. Изучить краткие теоретические сведения.

2. Установить операционную систему (ОС) Linux ROSA. Настроить ОС в режим маршрутизации методом форвардинга. Установить и настроить параметры Shorewall.

3. Соединить в виртуальной среде 3 ПК (см. рис. 12). Назначить IP-адреса формата 192.168.1.* и 192.168.1.*+100 для интерфейсов e1 и e2 соответственно; 192.168.2.* и 192.168.2.*+100 для интерфейсов e3 и e4 соответственно, где * - порядковый номер студента по журналу группы. Маска для обеих подсетей: 255.255.255.0

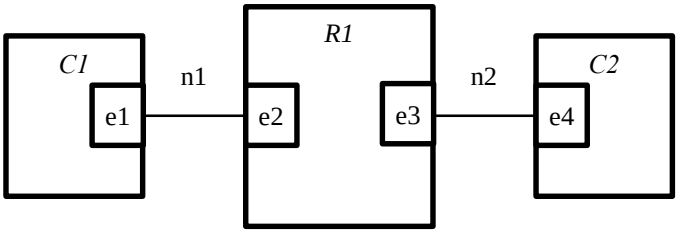

Рис. 12. Схема соединения ПК

где, e1-e4 – сетевые интерфейсы,

R1 – маршрутизатор,

C1 – контроллер домена (сервер),

C2 – подчиненный ему виртуальный ПК (клиент)

n1, n2 – имена виртуальных сетей.

4. В отчете указать данные для каждого интерфейса: назначенные IP- и физические адреса.

5. Создать макрос правил для передачи информационных потоков для файервола с именем Makros*, где * - порядковый номер студента по журналу группы. Макрос должен включать все подпункты из таблицы заданий. Проверить работу правил, заданных макросом, вручную. Продемонстрировать преподавателю. Варианты задания см. в табл. 6.

6. Составить отчет о проделанной работе.

Таблица 6

Варианты задания на настройку файервола

№ по журналу	№ варианта	Задание
1	**2**	**3**
1, 16	1.	Организовать доставку эхо-пакетов от маршрутизатора к серверу. Разрешить доступ к сетевой папке от сервера к клиенту.
2, 17	2.	Организовать доставку эхо-пакетов от сервера к маршрутизатору. Разрешить доступ к DNS серверу клиенту.
3, 18	3.	Организовать доставку эхо-пакетов от клиента к серверу. Разрешить доступ клиенту к ADDS (проверить включением в домен).
4, 19	4.	Организовать доставку эхо-пакетов от сервера к клиенту. Разрешить доступ клиенту к DHCP серверу.
5, 20	5.	Организовать доставку эхо-пакетов от маршрутизатора к клиенту. Разрешить доступ клиенту к ADDS.
6, 21	6.	Организовать доставку эхо-пакетов от клиента к маршрутизатору. Запретить доступ клиенту к ADDS.
7, 22	7.	Разрешить доставку DHCP пакетов между сервером и клиентом. Запретить DNS запросы от клиента к серверу.
8, 23	8.	Разрешить все эхо-запросы, кроме клиентских. Запретить DNS запросы от сервера к клиенту.
9, 24	9.	Разрешить все эхо-запросы, кроме серверных. Разрешить доступ к сетевой папке от клиента к серверу.
10, 25	10.	Разрешить все эхо-запросы. Разрешить доступ к сетевой папке от клиента к серверу и наоборот.
11, 26	11.	Разрешить все эхо-запросы, кроме от клиента к интерфейсу e2. Разрешить доступ к сетевой папке клиента, запретить к сетевой папке сервера.
12, 27	12.	Разрешить все эхо-запросы, кроме от сервера к интерфейсу e3. Разрешить доступ к сетевой папке сервера, запретить к сетевой папке клиента.

Окончание табл. 6

1	2	3
13, 28	13.	Запретить все эхо-запросы. Разрешить доступ ко всем сетевым папкам.
14, 29	14.	Запретить все эхо-запросы, кроме клиентских. Разрешить доступ к DHCP интерфейсу e2.
15, 30	15.	Запретить все эхо-запросы, кроме серверных. Разрешить доступ к DHCP интерфейсу e3.

Вопросы для контроля

1. Основы работы в сети и анализ сети
2. Понятие программный сокет и его назначение
3. Понятие маршрутизации, NAT, FORWARDING.
4. Понятие файервол, брандмауэр.
5. Порядок настройки маршрутизатора в среде Linux.
6. Что такое Shorewall?
7. Порядок настройки Shorewall.
8. Что такое макрос? Макроподстановка?
9. Какой формат макроса Shorewall?
10. Каков порядок написания правил в Shorewall?
11. Каков порядок настройки сетевых интерфейсов?
12. Каков порядок и синтаксис создания своих скриптов Shorewall в среде Linux?

Лабораторная работа № 4

СРЕДЫ ВИРТУАЛИЗАЦИИ. НАСТРОЙКА, АДМИНИСТРИРОВАНИЕ

Цель работы: изучить и освоить практически создание, настройки и администрирование систем аппаратной и программной виртуализации.

Основные сведения

Понятие виртуализации и ее виды

Виртуализация позволяет параллельно использовать на одном компьютере несколько операционных систем. Эта возможность очень востребована на практике: можно установить Linux в Windows, выполнять Windows в Linux, тестировать новую альфа-версию дистрибутива *xyz*, не опасаясь повредить действующую (стабильную) версию Linux, уверенно отделять друг от друга функции сервера (виртуализация сервера) и т. д.

Технологии виртуализации

Гость и хозяин. При описании систем виртуализации закрепилась метафора, рассматривающая основную систему как хозяина (host), а работающие на ней виртуальные машины как гостей (guests).

Технологии. Существуют различные методы виртуализации операционных систем. В следующем списке перечислены наиболее распространенные из них и названы некоторые программы (фирмы), которые пользуются этими технологиями.

Полная виртуализация (виртуальные машины, эмуляция). В данном случае программа имитирует работу виртуального аппаратного обеспечения, то есть компьютера, состоящего из процессора, ОЗУ, жесткого диска, сетевой карты и т. д. Гостевые системы «считают», что виртуальное аппаратное обеспечение является реальным. Чтобы такая система функционировала, работающая на хозяине программа виртуализации должна отслеживать код гостя и заменять определенные команды другими фрагментами кода. Эту задачу выполняет гипервизор (Virtual Machines Monitor, VMM — «монитор виртуальных машин»). Такая программа-гипервизор также отвечает за события, связанные с хранением информации и управлением процессами.

Преимущества: на виртуальной машине может функционировать практически любая операционная система. При этом в операционную систему не требуется вносить никаких изменений.

Недостатки: работает сравнительно медленно.

Программы/фирмы: VMware, QEMU, Parallels, VirtualBox, Microsoft Virtual PC.

Паравиртуализация. В данном случае хозяин также же предоставляет виртуальные машины, на которых выполняются программы гостей. Отличие от полной виртуализации состоит в том, что гостевую операционную систему для виртуализации требуется модифицировать, после чего эта система напрямую сообщается с VMM.

Преимущества: высокая эффективность.

Недостатки: требует специальной модификации операционных систем для целей виртуализации. Для такой системы с открытым кодом, как Linux, это не составляет никакой проблемы, чего не скажешь о коммерческих операционных системах, например, Windows. (В этой области налажена совместная работа между Xen и Microsoft или Novel и Microsoft, поэтому вероятно, что в будущем появятся версии Windows Server, оптимизированные специально под Xen.)

Программы/фирмы: Xen, UML (Linux в пользовательском режиме).

(Пара)виртуализация с поддержкой аппаратного обеспечения. Современные процессоры производства Intel и AMD содержат аппаратные функции, предназначенные для упрощения процессов виртуализации. В Intel такая технология называется Intel-VT (ранее — Vanderpool), а в AMD — AMD-V (ранее — Pacifica).

Преимущества: высокая эффективность, при некоторых вариантах внедрения не требуется вносить изменения в операционную систему.

Недостатки: необходимы специальные процессоры.

Программы/фирмы: KVM, Xen.

Виртуализация на уровне операционной системы (контейнеры). При использовании данного метода настоящие виртуальные машины не применяются. Вместо этого при таком подходе машины применяют общее ядро и фрагменты файловой системы хозяина. К важнейшим задачам системы виртуализации относится, в частности, обеспечение изоляции между хозяином и гостями для исключения каких бы то ни было проблем с безопасностью.

Достоинства: очень эффективна, сберегает ресурсы (ОЗУ, дисковое пространство и т. д.).

Недостатки: может применяться только тогда, когда хозяин и гости используют в точности одну и ту же операционную систему и совершенно одинаковую версию ядра. Операционная система должна быть модифицирована соответствующим образом.

Программы/фирмы: OpenVZ, Virtuozzo, Linux-VServer.

Все перечисленные методы, кроме первого, требуют внесения изменений в ядро, причем соответствующие операции производятся через Linux. В настоящее время, по крайней мере официально, в состав ядра входят только те функции виртуализации, которые относятся к KVM и UML. При использовании других методов ядро необходимо модифицировать с помощью неофициальной заплатки. Если, например, вы работаете с Xen-образным дистрибутивом, то знайте, что дистрибьютор заблаговременно встраивает в ядро функции, необходимые для работы в Xen.

Виртуальное аппаратное обеспечение

Эмулирование виртуального аппаратного обеспечения — это очень сложный процесс. В зависимости от механизма виртуализации или варианта его внедрения вы рано или поздно столкнетесь с границами возможностей вашего компьютера.

ОЗУ. Память компьютера должна быть достаточно объемной, чтобы выполнять все требования ресурсов хозяина и гостей, работающих на нем. Чем больше систем должны функционировать одновременно, тем больше оперативной памяти требуется. Например, на компьютере, которым я пользуюсь для тестирования, объем оперативной памяти достигает 6 Гбайт. Этого достаточно, чтобы без проблем работать одновременно в 6–7 дистрибутивах Linux.

Жесткий диск. Большинство систем виртуализации сохраняют файловые системы гостей в большом файле в системе хозяина. Таким образом, гости получают доступ к файлам жесткого диска не прямо, а опосредованно, через систему виртуализации. Следовательно, доступ к файлам в «гостевой» системе осуществляется значительно медленнее, чем в системе хозяина, в 2–3 раза.

CD/DVD-приводы. CD- и DVD-приводы выделяются хозяином гостям. В любом случае предоставляется доступ «только для чтения». Мне не известна ни одна система виртуализации, которая позволяла бы записывать CD и DVD в гостевой системе.

Большинство программ виртуализации дают возможность присвоить каждому виртуальному CD или DVD ISO-файл. Тогда гость вместо того, чтобы пользоваться реальным приводом, обращается к такому файлу. Это исключительно полезно в тех случаях, когда необходимо многократно устанавливать одни и те же программы. При необходимости вы можете без особого труда сами извлечь ISO-файл с CD или DVD.

Графический адаптер. Для более или менее эффективного использования графических возможностей на каждой гостевой системе необходимо установить специальный драйвер, настроенный на виртуализационное ПО хозяина. В зависимости от применяемой системы виртуализации существуют определенные ограничения в области использования трехмерной графики.

Звуковые функции. Большинство программ виртуализации предоставляют гостевой системе виртуальную звуковую карту и перенаправляют звуковой вывод на аудиосистему хозяина. Если вы не выдвигаете экстраординарных требований к аудиосистеме (например, вам не требуется эффект «звук вокруг»), то такого механизма вполне достаточно.

USB-устройства и внешнее аппаратное обеспечение. Ввод, осуществляемый с помощью клавиатуры и мыши, направляется из системы-хозяина в систему-гость. От применяемой системы виртуализации зависит, к каким внешним устройствам будут иметь доступ пользователи гостевых машин. USB-устройства, к сожалению, поддерживаются не всеми системами виртуализации, а если и поддерживаются, то с серьезными ограничениями.

Программы для виртуализации

Спектр предлагаемых инструментов виртуализации, как в коммерческом сегменте, так и среди свободно распространяемого ПО, необозримо велик. В следующем списке кратко рассмотрены важнейшие флагманы рынка виртуализации. В скобках указано, является ли данный продукт коммерческим или распространяется свободно, какая фирма занимается разработкой и реализует на рынке соответствующую продукцию.

1. VMware (коммерческий, EMC). Фирма VMware — бесспорный лидер на рынке программ для виртуализации. Список производимой ею продукции начинается с пользовательских программ для ПК (рабочая станция и проигрыватель VMware) и заканчивается рядом мощных программ для сервера (VMware Server, ESXi, vSphere). Отдельные программы распространяются бесплатно, но не с открытым кодом. В качестве системы-хозяина поддерживаются Windows, Linux, а в отдельных случаях и Mac OS X. Некоторые продукты VMware работают вообще без операционной системы, «с нуля» (bare metal).

2. VirtualBox (частично бесплатная программа, Sun/Oracle). Функции программы VirtualBox в целом похожи на функции рабочей станции VMware, таким образом VirtualBox также подходит для настольной виртуализации. В качестве системы-хозяина поддерживаются Windows,

Linux и Mac OS X. Для частных пользователей программа VirtualBox бесплатна; кроме того, есть свободно распространяемая версия этой программы, которая может использоваться и коммерческим образом, на условиях стандартной общественной лицензии (GPL). VirtualBox исключительно быстро развивалась в последние годы. Такой факт, что за год выходило несколько версий программы, говорит о том, что VirtualBox хорошо совместим с новейшими версиями ядра и X-версиями.

3. KVM/QEMU (свободно распространяемая программа, Red Hat). Собственно, KVM — это просто модуль ядра, который радикально ускоряет работу эмулятора QEMU при использовании современных процессоров, при том что раньше этот эмулятор работал достаточно медленно. С тех пор как KVM официально вошел в состав ядра, а Red Hat купил Qumranet — фирму, разработавшую KVM, — значение модуля KVM резко выросло и он уже считается стандартным виртуализационным решением в дистрибутивах Fedora, Ubuntu и, конечно же, для версии 6 Red Hat Enterprise Linux. KVM одинаково хорош для применения как на ПК, так и на сервере. И все же по таким показателям, как понятность для пользователей, совместимость и скорость, KVM пока не может конкурировать с аналогичными коммерческими программами — Vmware, VirtualBox и Xen. В качестве системы-хозяина поддерживается только Linux.

4. Xen (частично бесплатная программа, Citrix). Xen — это гипервизор, функционирующий без операционной системы. Виртуализированные гостевые системы работают в так называемых доменах (domU), причем первый домен имеет особые привилегии и в определенном смысле сравним с системой-хозяином в других программах виртуализации. Во многих практических ситуациях Xen значительно эффективнее, чем другие системы виртуализации. Однако в то же время настройка и конфигурирование гостевых систем (доменов) требует гораздо больших усилий. Это не в последнюю очередь объясняется тем, что расширения ядра, необходимые для правильной работы Xen, очень объемны и, несмотря на все приложенные усилия, пока не входят в состав официальной версии ядра. Если же вы готовы вложить в работу с Xen много времени, то достигнете выдающихся результатов, но для использования от случая к случаю Xen не годится.

5. OpenVZ и Virtuozzo (частично бесплатные программы, Parallels), а также Linux-VServer (свободно распространяемое ПО). OpenVZ, базирующийся на его основе коммерческий продукт Virtuozzo и технически

сходное виртуализационное решение Linux-VServer позволяют обустраивать много изолированных сред в одном дистрибутиве Linux. OpenVZ или Virtuozzo при работе исходят из того, что в системах «хозяина» и его «гостей» работает одна и та же версия Linux. Эта концепция отлично подходит для тех случаев, когда необходимо виртуализировать несколько (много!) аналогичных серверов. Такая система частично используется провайдерами интернет-хостинга, которые предлагают недорогие виртуальные корневые серверы.

6. Hyper-V (коммерческая программа, Microsoft). Корпорация Microsoft поначалу не успела поучаствовать в разделе рынка виртуализации, но сейчас прилагает титанические усилия, чтобы сделать собственное виртуализационное решение Hyper-V конкурентоспособным. Hyper-V воспринимает систему Windows Server как систему-хозяина, но при этом может поддерживать Linux в качестве гостевой системы. Компания даже разработала для этой цели собственные драйверы ядра Linux, причем эти драйверы с открытым кодом (такой шаг дался Microsoft с большим трудом, так как эта корпорация очень долго представляла Стандартную Общественную Лицензию в самом черном свете).

VMware ESXi

VMware ESXi является сервером аппаратной виртуализации ОС. Часто используется в современных компьютерных парках организаций, а также позволяет сэкономить материальные затраты на приобретение дополнительных ОС семейства Windows, так как имеет договоренности с компанией Microsoft об использовании одной лицензии на 4 виртуальных машинах.

Аппаратная виртуализация доступна только на оборудовании, поддерживающем соответствующие функции, полную поддержку которых гарантирует фирма Intel.

Также данная среда аппаратной виртуализации способна работать с внешними контроллерами и массивами данных, поддерживающих технологию RAID.

Управление виртуальным парком осуществляется через специальную утилиту – VSphere Hypervisor, версия которой должна точно соответствовать версии ESXi. Соединение с сервером происходит по защищаемому сертификатом каналу. Внешний вид ESXi представлен на рисунке 13.

Важным разделом функционирования любой среды является раздел настроек (см. рис. 14). Чтобы в него попасть, необходимо нажать F2 и ввести учетные данные, указанные при установке системы.

Здесь содержатся основные (корневые) настройки ESXi:

1. Configure Password – позволяет управлять паролем пользователя, под которым был выполнен вход.

2. Configure Manage Network – содержит настройки, касающиеся сетевого взаимодействия со средой ESXi. У каждой гостевой виртуальной машины сетевые настройки выставляются независимо от этих.

3. Troubleshooting Options – содержит настройки доступа к среде ESXi: с помощью консоли ESXi или с помощью SSH.

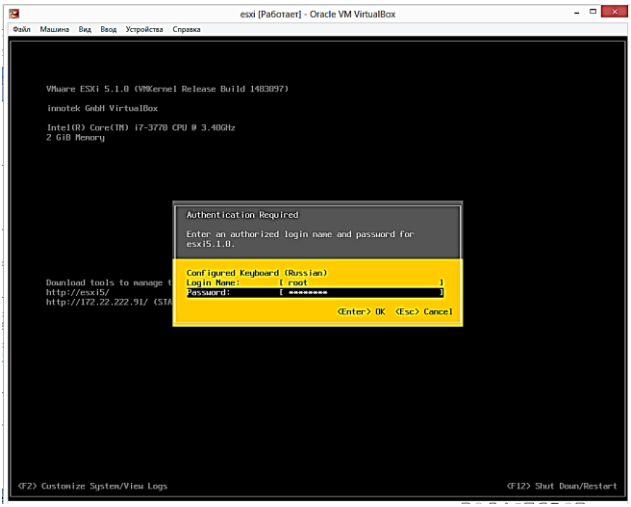

Рис. 13. Окно аутентификации ESXi

Дальнейшее управление виртуальным парком осуществляется через приложение VSphere Hypervisor. Внешний вид окна авторизации представлен на рис. 15.

В поле “IP address/Name” вводится адрес сервера ESXi, учетные данные – root. После входа в оболочку управления ESXi VSphere Hypervisor появится окно (см. рис. 16).

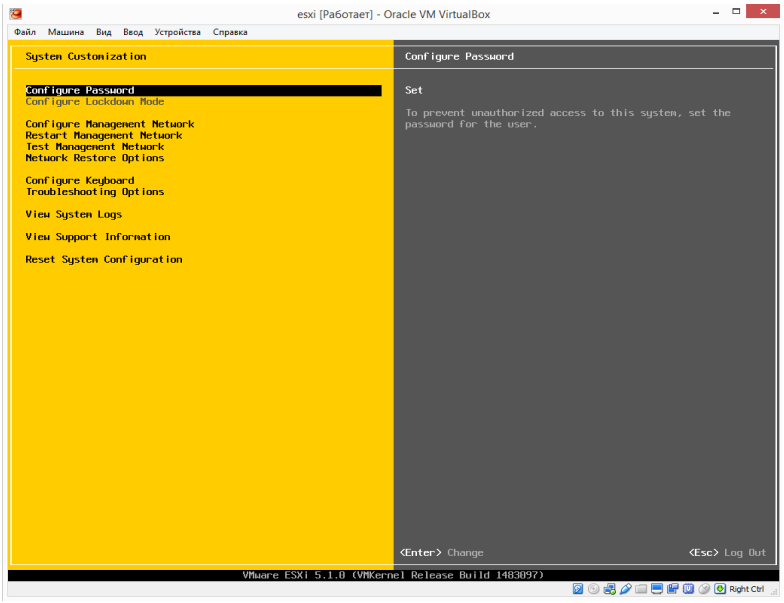

Рис. 14. Раздел настроек ESXi

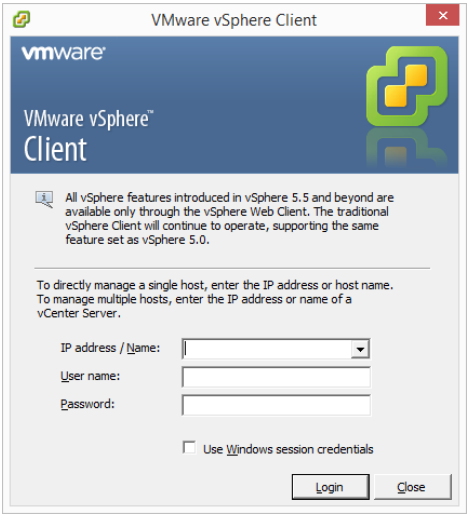

Рис.15. Авторизация в среде ESXi

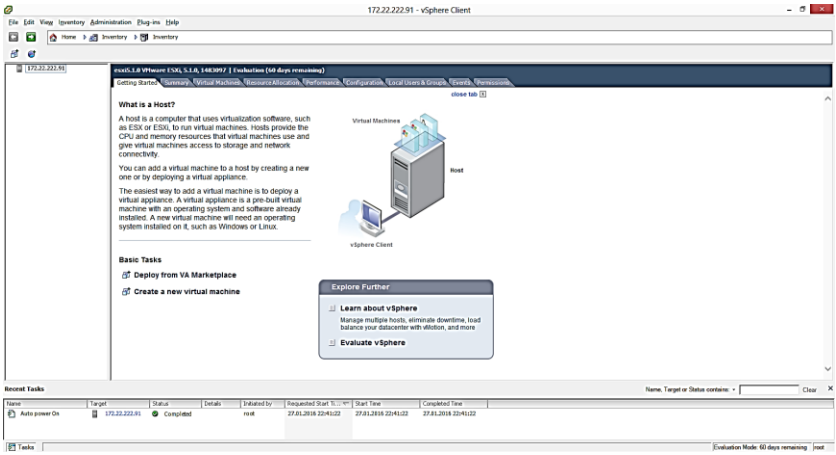

Рис.16. VSphere Hypervisor

В этой оболочке осуществляется полное управление виртуальным компьютерным парком: создание, настройка, администрирование и управление виртуальными машинами, управление аппаратными и сетевыми параметрами виртуальной среды в целом и каждой машины в частности и. т.д.

Также существует возможность создавать новых пользователей для управления отдельными виртуальными машинами или группами виртуальных машин, делегировать права управления и администрирования ими и много другое.

Содержание работы

1. Изучить краткие теоретические сведения.
2. Установить, настроить и проверить работу аппаратной виртуальной среды VMware-ESXi-5.1.0-update2. Для реализации использовать Virtual Box, профиль создать со следующими параметрами:
   1) ОС Linux Red Hat x64.
   2) ОЗУ 2 ГБ.
   3) Видеопамять - 12 МБ (режим управления консольный).
   4) HDD – 70 ГБ, тип фиксированный, *.vmdk.
   5) Два сетевых адаптера Intel Pro 1000 MT Desktop, неразборчивый режим: Разрешить все.
   6) CPU – не менее двух.

Обязательно проверить установку плагинов, соответствующих версии Virtual Box. Должна быть активна функция виртуализации процессора Intel Virtualization в BIOS хостовой машины, а также активны функции AMD-V/VT-X, Nested Paging, PAE-NX в Virtual Box.

3. Установить и проверить работу одной виртуальной машины в среде ESXi посредством VSphere Hypervisor под управлением ОС Windows.

4. Создать и настроить в среде VMware второй сетевой интерфейс и второй виртуальный коммутатор. Организовать доступ к виртуальной машине по двум сетевым интерфейсам: один в режиме «внутренняя сеть», а второй – «сетевой адаптер хоста». Добиться доступности виртуальной машины из хостовой ОС по сети, из виртуальной ОС Windows, установленной ранее (см. рис. 13, клиент). Проверку следует производить посредством команды Ping.

5. Продемонстрировать результат преподавателю.

6. Оформить отчет о проделанной работе.

Вопросы для контроля

1. Понятие виртуализации и ее виды.
2. Технологии виртуализации. Полная виртуализация (виртуальные машины, эмуляция).
3. Технологии виртуализации. Паравиртуализация.
4. Технологии виртуализации. (Пара)виртуализация с поддержкой аппаратного обеспечения.
5. Технологии виртуализации. Виртуализация на уровне операционной системы (контейнеры).
6. Технологии виртуализации. Виртуальное аппаратное обеспечение.
7. Программы для виртуализации. VMware.
8. Программы для виртуализации. VirtualBox.
9. Программы для виртуализации. KVM/QEMU.
10. Программы для виртуализации. Xen.
11. Программы для виртуализации. OpenVZ и Virtuozzo.
12. Программы для виртуализации. Hyper-V.
13. Особенности настройки ESXi.
14. Особенности использования VSphere Hypervisor.
15. Настройки VSphere Hypervisor.
16. Создание виртуальных машин в VSphere Hypervisor.

Заключение

Сервис и сопровождение ИС — это практическая реализация методов управления ИС и соответствующих технологий ее поддержки. По мере роста организации и увеличения функций ИС требуется все больше времени и человеческих ресурсов для управления и сопровождения ИС.

Все новые компьютерные технологии используются при построении ИС, создавая большие возможности для реализации прикладных функций, но они усложняют и диверсифицируют ИС, при этом, чем больше повседневно используются современные, продвинутые компьютерные технологии, тем критичнее их надежность, для уверенности в корректной работе ИС требуется все более четкое и квалифицированное администрирование.

Постоянно происходит развитие моделей управления ИС и соответствующих протоколов стандартизирующими организациями и компьютерными сообществами обновляются или создаются стандарты в различных областях реализации ИС. Администратор системы (АС) должен владеть знаниями как существующих технологий и методов их администрирования, так и новых технологий, а также способами обеспечения их сосуществования со старыми технологиями. Поэтому управление ИС становится все более сложной проблемой даже для опытных профессионалов. А требования к системам управления и их сложность возрастают.

Следует подчеркнуть, что. несмотря на постоянное развитие технических средств, для служб администратора системы всегда останутся проблемы организационные и «политические», решение которых требует терпения и оптимизма, а проблема постоянного повышения квалификации и компетенции администратора системы в безграничной области информационных технологий останется ключевой.

Библиографический список

1. **Беленькая М.Н., Малиновский С.Т., Яковенко Н.В.** Администрирование в информационных системах. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2011. - 400 с., ил. - ISBN 978-5-9912-0164-3.
2. **Кофлер М.** Linux. Установка, настройка, администрирование. - СПб.: Питер, 2014. - 768 с.: ил. - ISBN 978-5-496-00862-4.
3. **Моримото, Рэнд, Ноэл, Майкл, Ярдени, Гай, и др.** Microsoft Windows Server 2012. Полное руководство. : Пер. с англ. — М.: ООО "И.Д. Вильямс", 2013. - 1456 с. : ил. — Парал. тит. англ. - ISBN 978-5-8459-1848-2 (рус.).

Учебное издание

Сосин Андрей Иванович

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Лабораторный практикум