Лабораторная работа №2
Механизмы резервного копирования данных в операционной системе Windows 2003 Server и Windows 2008 R2 Server.

Цель работы: Получить навыки архивирования и восстановления системы, используя стандартные утилиты Windows Server 2003 и Windows Server 2008. Решить задачи сетевого администратора связанные с сохранением, архивированием информации, и ее последующим восстановлением.

Дано: Имеется локальная сеть с контроллером домена на базе ОС Windows 2003 Server или Windows Server 2008.
Задание: Необходимо, используя стандартные утилиты Windows Server 2003 или Windows Server 2008 обеспечить архивирование и восстановления системы, а также настроить механизмы резервирования важных данных.

Краткие теоретические сведенья:
Ни один носитель информации не является абсолютно надежным, из строя может выйти любое устройство хранения данных, и данные могут быть потеряны. Кроме аппаратных сбоев возможна также потеря данных по причине действия вредоносных программ (вирусы и т.п.). А самая распространенная причина порчи или удаления данных — ошибки пользователей (как обычных, так и администраторов), которые могут по ошибке удалить или перезаписать не тот файл.

По этой причине возникает необходимость регулярного создания резервных копий информации — файлов с документами, баз данных и состояния операционной системы.

Системы семейства Windows Server имеют встроенный инструмент создания резервных копий — утилиту *ntbackup*. Данная утилита позволяет сохранять резервные копии на самых различных носителях — ленточных накопителях, магнитооптических дисках, жестких дисках (как на локальных дисках данного сервера, так и на сетевых ресурсах, размещенных на других компьютерах сети). В версии системы Windows 2003 реализован механизм т.н. теневых копий *Shadow Copy*, который заключается в том, что в начале процедуры архивации система делает моментальный «снимок» архивируемых файлов и уже после этого создает резервную копию из этого снимка. Данная технология позволяет архивировать файлы, которые в момент запуска утилиты *ntbackup* были открыты пользователями.
Сетевой администратор должен совместно с пользователями определить те данные, которые нужно регулярно архивировать, спланировать ресурсы, необходимые для создания резервных копий, составить расписание резервного копирования, настроить программу резервного копирования и планировщик заданий для автоматического создания резервных копий. Кроме этого, в задачу сетевого администратора входит также регулярное тестирование резервных копий и пробное восстановление данных из резервных копий (чтобы вовремя обнаружить возникающие проблемы в создании резервных копий).

Архивирование и восстановление файловых ресурсов. Базовые понятия службы резервного копирования
Все операции по созданию резервных копий и восстановлению данных в ОС семейства Windows осуществляются утилитой *ntbackup*.

Рассмотрим основы резервного копирования файловых ресурсов. Каждый файл, хранящийся на диске компьютера, независимо от типа файловой системы, имеет атрибут *archive*, который в Свойствах файла отображается как «*Файл готов для архивирования*» (откройте Свойства файла и нажмите кнопку «*Другие*»). Если в Свойствах файла вручную убрать галочку у этого атрибута, то при любом изменении в файле операционная система автоматически снова установит этот атрибут. На использовании изменений данного атрибута основаны все используемые в системе Windows методики резервного копирования.

Типы резервного копирования Windows Server 2003
Утилитой *ntbackup* можно создавать резервные копии различных типов. Рассмотрим их отличительные особенности и различные варианты их применения.

Обычный (Normal)
При выполнении данного типа архивирования утилита *ntbackup* архивирует все файлы, отмеченные для архивации, при этом у всех заархивированных файлов очищается атрибут «Файл готов для архивирования». Данный вид архивирования необходим для создания еженедельных полных резервных копий каких-либо больших файловых ресурсов. Если в компании или организации имеются достаточные ресурсы, то можно ежедневно осуществлять полное архивирование данных.

Разностный (Differential)
При выполнении Разностного архивирования утилита *ntbackup* из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для архивирования», при этом данный атрибут не

очищается. Использование Обычного и Разностного архивирования позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий. Например, если раз в неделю (как правило, в выходные дни) создавать Обычные копии, а в течение недели ежедневно (как правило, в ночное время) — Разностные, то получается выигрыш в объеме носителей для резервного копирования. При такой комбинации архивирования «Обычный + Разностный» процесс восстановления данных в случае утери информации потребует выполнения двух операций восстановления — сначала из последней Полной копии, а затем из последней Разностной резервной копии.

Добавочный (Incremental)
При выполнении Добавочного архивирования утилита *ntbackup* из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для архивирования», при этом данный атрибут очищается. Использование Обычного (раз в неделю по выходным) и Добавочного (ежедневно в рабочие дни) архивирования также позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий. Но процесс восстановления данных при использовании комбинации «Обычный + Добавочный» уже будет выполняться иначе: в случае утери информации для восстановления данных потребуется сначала восстановить данные из последней Полной копии, а затем последовательно из всех Добавочных копий, созданных после Полной копии.

Копирующий (Copy)
При таком типе архивирования утилита *ntbackup* заархивирует все отмеченные файлы, при этом атрибут «Файл готов для архивирования» остается без изменений.

Ежедневный (Daily)
Ежедневный тип архивирования создает резервные копии только тех файлов, которые были модифицированы в день создания резервной копии.

Два последних типа не используются для создания регулярных резервных копий. Их удобно применять в тех случаях, когда с какой-либо целью нужно сделать копию файловых ресурсов, но при этом нельзя нарушать настроенные регулярные процедуры архивирования.

Разработка и реализация стратегии резервного копирования. Понятие плана архивации
Создание и реализация плана архивации и восстановления информации — непростая задача. Сетевому администратору надо определить, какие данные требуют архивации, как часто проводить архивацию и т. д.
При создании плана ответьте на следующие вопросы:

- Насколько важны данные? Этот критерий поможет решить, как, когда и какую информацию архивировать. Для критичной информации, например, баз данных, следует создавать избыточные архивные наборы, охватывающие несколько периодов архивации. Для менее важной информации, например, для текущих пользовательских файлов, сложный план архивации не нужен, достаточно регулярно сохранять их и уметь легко восстанавливать.
- К какому типу относится архивируемая информация? Тип информации поможет определить необходимость архивации данных: как и когда данные должны быть сохранены.
- Как часто изменяются данные? Частота изменения влияет на выбор частоты архивирования. Например, ежедневно меняющиеся данные необходимо сохранять каждый день.
- Нужно ли дополнить архивацию созданием теневых копий? При этом следует помнить, что теневая копия — это дополнение к архивации, но ни в коем случае не ее замена.
- Как быстро нужно восстанавливать данные? Время — важный фактор при создании плана архивации. В критичных к скорости системах нужно проводить восстановление очень быстро.
- Какое оборудование оптимально для архивации и есть ли оно у вас? Для своевременной архивации вам понадобится несколько архивирующих устройств и несколько наборов носителей. Аппаратные средства архивации включают ленточные накопители (это наименее дорогой, но и самый медленный тип носителя), оптические диски и съемные дисковые накопители.
- Кто отвечает за выполнение плана архивации и восстановления данных? В идеале и за разработку плана, и собственно за архивацию и восстановление должен отвечать один человек.
- Какое время оптимально для архивации? Архивация в период наименьшей загрузки системы пройдет быстрее, но не всегда возможно провести ее в удобные часы. Поэтому с особой тщательностью архивируйте ключевые данные.
- Нужно ли сохранять архивы вне офиса? Хранение архивов вне офиса — важный фактор на случай стихийного бедствия. Вместе с архивами сохраните и копии ПО для установки или переустановки ОС.

Для построения правильной и эффективной системы резервного копирования необходимо детально изучить и задокументировать все файловые ресурсы, используемые в компании, а затем тщательно спланировать стратегию

резервного копирования и реализовать ее в системе. Для планирования стратегии необходимо ответить на следующие вопросы:

- какие именно ресурсы будут архивироваться;
- минимальный промежуток времени для восстановления данного ресурса при возникновении аварии;
- какой объем данных будет архивироваться;
- какова емкость носителей для хранения резервных копий и скорость записи на эти носители;
- сколько времени будет занимать архивирование каждого ресурса;
- как часто будет производиться архивация каждого ресурса;
- если резервные копии записываются на ленты, то как часто будет производиться перезапись лент;
- по какому графику будет производиться тестовое восстановление данных.

При ответе на эти вопросы будет спланирована потребность в количестве и емкости накопителей и устройств для выполнения резервных копий, требования к пропускной способности сети для создания резервных копий, график выполнения резервного копирования, план восстановления на случай аварии.

Выбор архивных устройств и носителей

Определив, какие данные и как часто архивировать, можно выбрать аппаратные средства архивации и необходимые носители. Инструментов для архивации данных множество. Одни быстрые и дорогие, другие — медленные и надежные. Выбор подходящего оборудования для организации зависит от многих факторов.

- Емкость — количество регулярно архивируемых данных. Справится ли оборудование с нагрузкой в отведенное время?
- Надежность аппаратных средств и носителей. Можете ли вы пожертвовать надежностью ради экономии или скорости?
- Расширяемость решения. Удовлетворяет ли ваше решение потребностям роста организации?
- Скорость архивации и восстановления. Можете ли вы пожертвовать скоростью ради снижения стоимости?
- Цена архивации. Приемлема ли она для вашего бюджета?

Типовые решения архивации

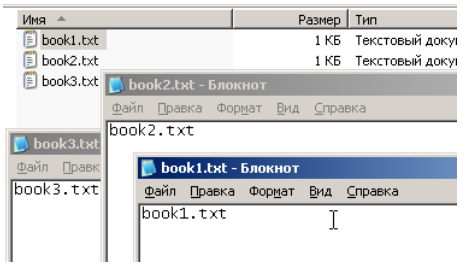
Итак, на план архивации влияют емкость, надежность, расширяемость, скорость и цена. Определив, какие из этих факторов наиболее важны для вашей организации, вы примете подходящее решение. Вот некоторые общие рекомендации:

- Ленточные накопители — самые распространенные устройства архивации. Данные хранятся на кассетах с магнитной лентой. Лента относительно недорога, но не особенно надежна: она может помяться или растянуться, с течением времени — размагнититься и перестать считываться. Средняя емкость кассет с лентой варьируется от единиц до десятков Гбайт. По сравнению с другими решениями ленточные накопители довольно медленны. Их достоинство — невысокая цена.
- Накопители на цифровой ленте (digital audio tape, DAT) — пришли на смену традиционным ленточным накопителям. Существует несколько форматов DAT, их емкости составляют 35 и 260 Гбайт.
- Ленточная библиотека с автозагрузкой — устройство для создания расширенных архивных томов на нескольких лентах, которых хватает для нужд всего предприятия. Ленты набора в процессе архивации или восстановления данных автоматически меняются. В большинстве таких библиотек применяются DAT-ленты. Их главный «*минус*» — высокая цена.
- Магнитооптические накопители с автозагрузкой подобны ленточным библиотекам, только вместо лент в них используются магнитооптические диски. Цена также очень высока.
- Съемные диски, например Iomega Jazz емкостью 1-2 Гбайт, все чаще используются в качестве устройств архивации. Они обладают хорошей скоростью и удобны в работе, но стоят дороже ленточных или DAT-накопителей.
- Дисковые накопители обеспечивают наивысшую скорость при архивации и восстановлении файлов. Если при архивации на ленту вам потребуются часы, то дисковый накопитель позволяет завершить процесс за несколько минут. К недостаткам дисковых накопителей следует отнести относительно высокую цену.

Ход работы:

Создания задания на выполнения архивации данных

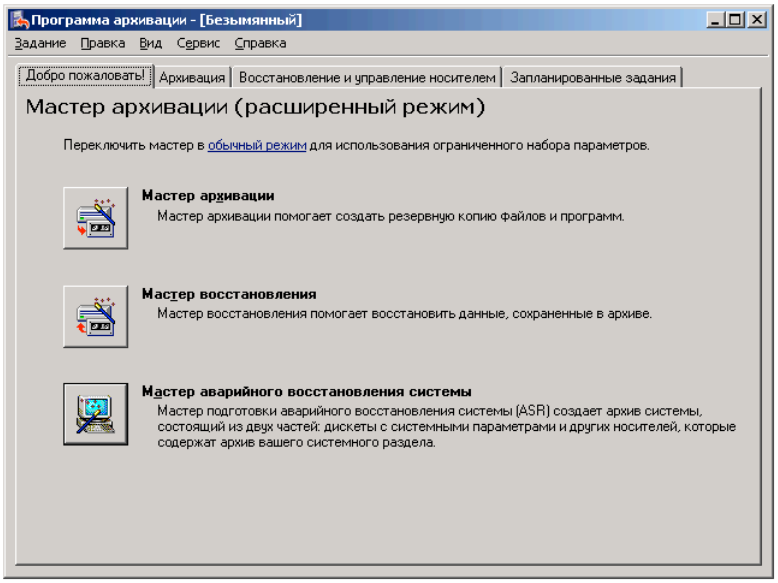
1. Создать на диске «C» Вашего сервера каталог *backup* и *restore*;
2. В папке library, созданной в одной из предыдущих работ создать 3 текстовых файла с наименованиями *book1.txt*, *book2.txt* и *book3.txt*. Файлы должны содержать свое наименование.



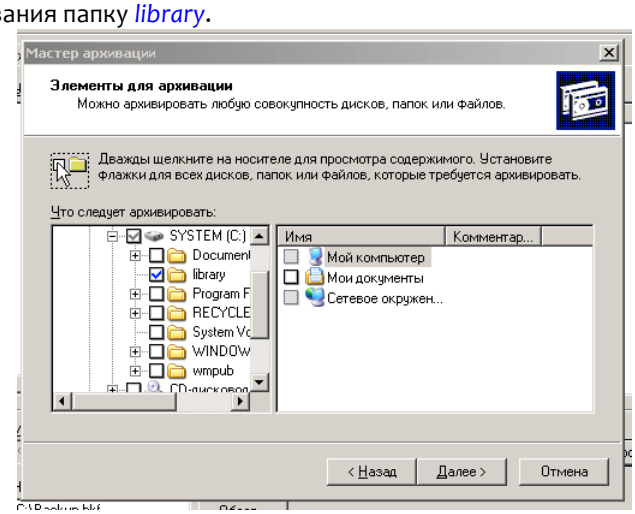
3. Запустить утилиту резервного копирования *ntbackup*.

Эту утилиту можно запустить из Главного меню системы (кнопка «Пуск» — «Все программы» — «Стандартные» — «Служебные» — «Архивация данных»), а можно запустить более быстро из командной строки (кнопка «Пуск» — «Выполнить» — «ntbackup» — кнопка «ОК»). При первом запуске утилиты рекомендуем убрать галочку у поля «Всегда запускать в режиме мастера».

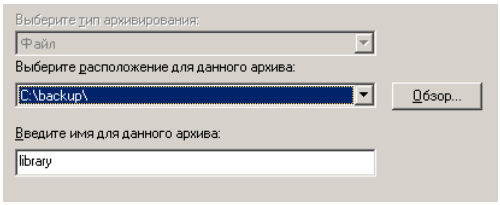
4. Запустить «Мастер архивации» (на закладке «Добро пожаловать» нажать кнопку «Мастер архивации».



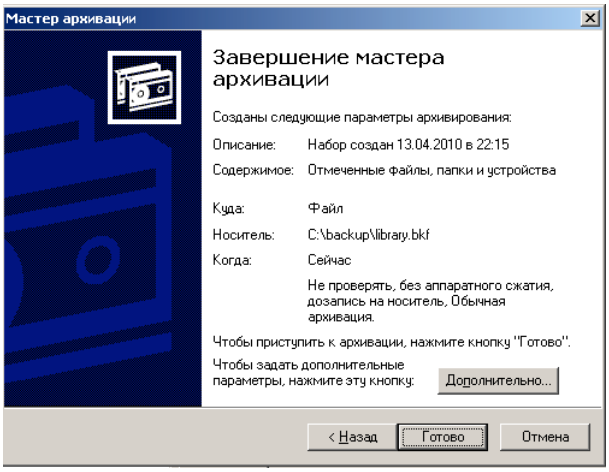
5. После запуска мастера нажмем кнопку «Далее» и выберем, что нам нужно архивировать, в данном примере — «Архивировать выбранные файлы, диски или сетевые данные»
6. Выберем для архивирования папку *library*.



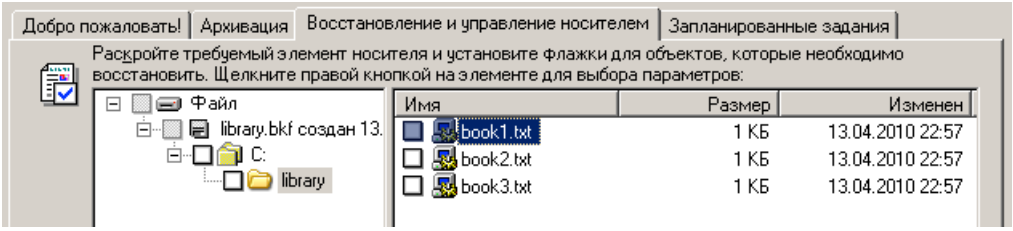
7. Выберем место для создания резервной копии, создадим файл с именем *library*, этому файлу автоматически будет назначено расширение «*.bkf*»



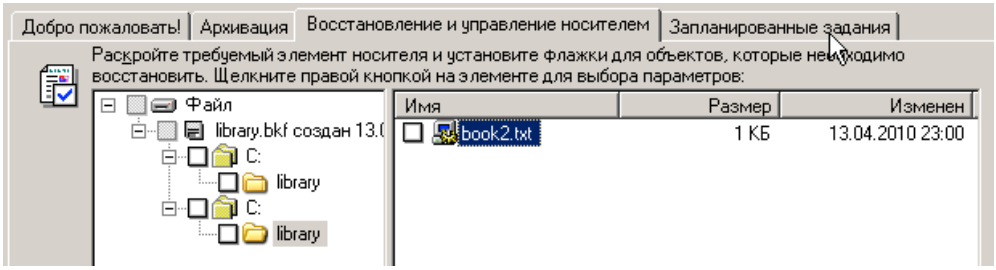
8. На данном этапе нажмем кнопку «Готово».



9. Проверяем полученный результат.



10. Вносим изменение в файл *book1.txt* и *book2.txt*, у файла *book1.txt* убираем атрибут «Файл готов для архивирования», а *book3.txt* - удаляем.
11. Запускаем снова процесс архивации, но на 8 этапе нажмем кнопку «Дополнительно», чтобы задать дополнительные параметры и выбираем тип архивации «Добавочный». Далее все пункты по умолчанию, но при этом не забывайте запоминать, что Вы делаете. Проверяем полученный результат. Почему он такой?



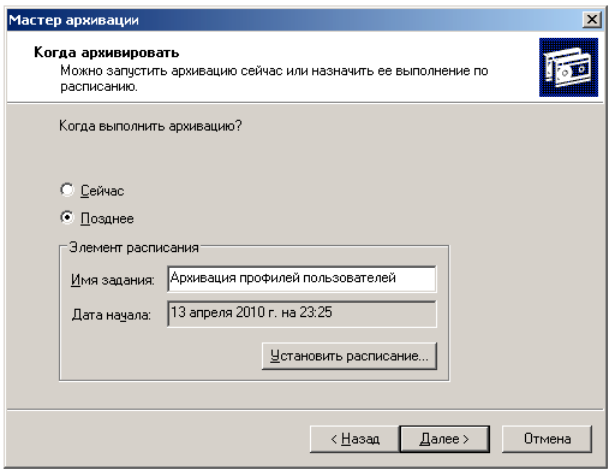
12. Восстановите файл *book3.txt*. Для этого выполните следующие действия:

- Запустим утилиту резервного копирования *ntbackup*.
- Перейдем на закладку "Восстановление и управление носителем".
- После появления в списке архивных файлов нужного архива раскроем этот архив и выберем файлы для восстановления из резервной копии. При этом мы можем восстановить файлы в то место, где они были ранее ("Исходное размещение") или выбрать иной путь для их сохранения ("Альтернативное размещение"). Выберите папку *restore*.
- После определения всех параметров восстановления нажмем кнопку "Восстановить", утерянные данные будут восстановлены.

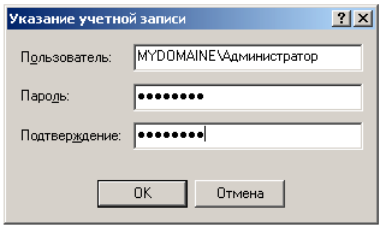
13. Создайте задания на выполнения архивации данных для папки *profiles*, используя выбор дополнительных возможностей:

- Выбираем тип архивирования (выберем «Обычный»).

- Ничего не меняем на странице «Способы архивации».
- На странице «Параметры архивации» можно выбрать замену существующих архивов или добавление архива (если файл с архивной копией уже существует).



14. На странице «Когда архивировать» задайте расписание для автоматического создания резервной копии — выберите вариант «Позднее» и задайте расписание архивирования, чтобы архивирование происходило по всем рабочим дням недели. Время начала установите, исходя из текущего времени системы + пять минут.
15. Нажмите далее. Система запросит имя и пароль пользователя, с чьими полномочиями будет выполняться задание архивирования. Рекомендуем для выполнения заданий резервного копирования создать специальные учетные записи, обладающие достаточными правами (как минимум члены группы «Операторы архива»).



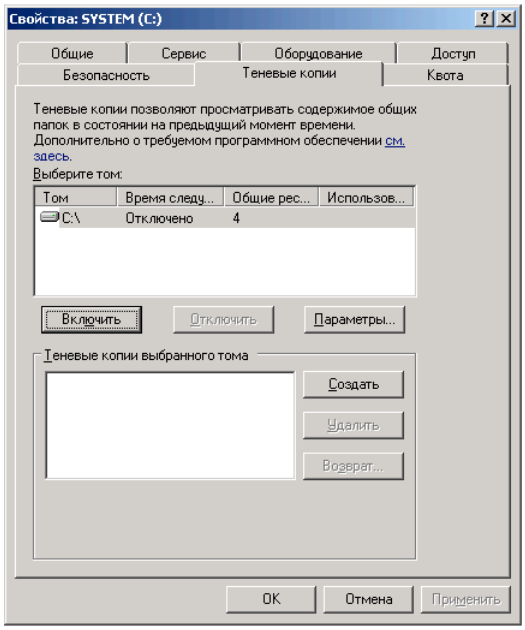
16. Нажмем кнопку «Готово», задание будет создано, и оно появится в списке «Назначенных заданий». Теперь оно будет выполняться регулярно в соответствии с расписанием.
17. Завершите сеанс администратора, ожидайте до завершения задания. После проверьте результат.

Теневые копии

Эта технология, реализованная в Windows 2003, позволяет архивировать открытые файлы с помощью создания «снимка» файловых ресурсов. По умолчанию теневые копии создаются на том же томе, где хранятся сетевые папки, поэтому они не смогут стать серьезной защитой от аппаратных аварий (например, выход из строя диска, на котором размещены эти данные). Можно настроить создание теневых копий на другом томе, что повысит уровень защиты. Теневые копии позволяют восстанавливать данные, ошибочно удаленные или модифицированные пользователями. При этом пользователи могут восстанавливать данные сами, без участия системного администратора. Теневые копии создаются только на томах с файловой системой NTFS.

Рассмотрим пример создания и использования теневых копий тома.

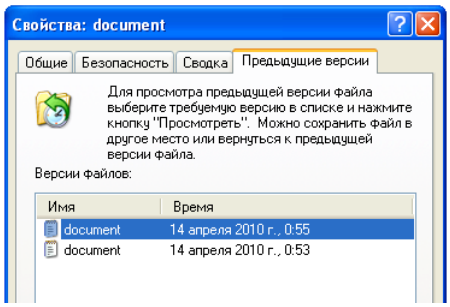
1. Создадим в сетевой папке на сервере файл *document.txt*, содержащий текст: «11111».
2. Откроем Свойства какого-либо тома и перейдем на закладку «Теневые копии». По умолчанию создание теневых копий для всех томов отключено.
3. Включим создание теневых копий для тома «С». При этом автоматически создастся первая теневая копия. В этом окне также можно вручную создать теневую копию данного тома в любой момент времени.



4. Настроим параметры теневого копирования. Для хранения теневых копий на томе требуется не менее 100 МБ дискового пространства, на каждом томе создается максимум 64 копии.
5. Настройте размер пространства для хранения копий в размере 200МБ и расписание создания теневых копий — дважды в день в 14-00 и 24-00.
6. На клиентской машине откройте файл *document.txt* и добавьте новую строку «22222».
7. На сервере вручную создайте еще одну теневую копию данного тома.
8. На клиентской машине откройте файл *document.txt* и добавьте новую строку «33333».

***Замечание**. Теневые копии создаются не для всех файлов тома, а только для тех, которые размещены в папках, выставленных в сеть для общего доступа.*

Использование теневых копий. После создания теневых копий пользователю становятся доступны Предыдущие версии файлов. Для использования этих возможностей нужна клиентская часть для доступа к теневым копиям. В системе Windows 2003 клиентская часть уже имеется в системе, а для Windows 2000/XP ее нужно установить. Дистрибутив клиента теневых копий хранится на сервере в папке «%SystemRoot%\system32\clients\twclient», в файле twcli32.msi. При установленном клиенте в свойствах файла, открываемого из сетевых папок, становится доступна закладка «Предыдущие версии». Проверьте, доступна ли данная закладка в Вашей клиентской системе, если нет, то установите необходимое ПО.



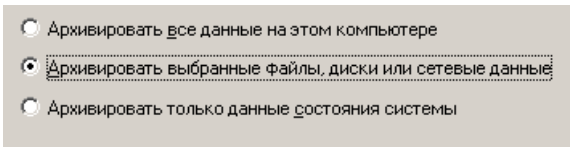
Пользователь теперь может просмотреть предыдущие копии, скопировать их в другой файл или восстановить содержимое файла в одно из предыдущих состояний. Закладка «Предыдущие версии» доступна в Свойствах не только конкретного файла, но и всей сетевой папки. Поэтому можно восстановить не только измененные файлы, но и ошибочно удаленные.

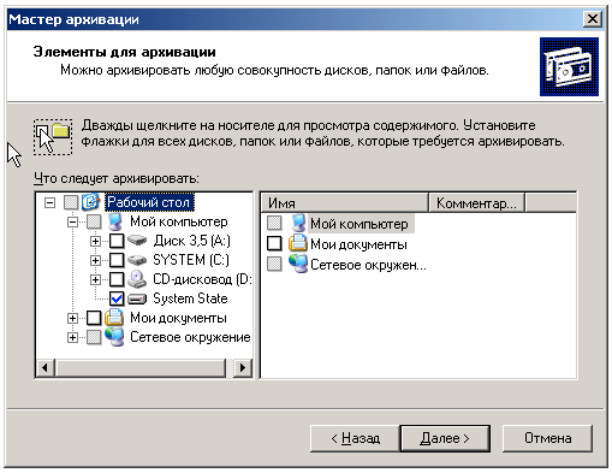
Архивирование и восстановление состояния системы

Большую часть работ по резервному копированию составляют задания на копирование бизнес-информации. Но имеется также возможность создания резервных копий для восстановления функционирования самой операционной системы. Есть два варианта архивирования системных данных — архивирование состояния системы (*System State*) и создания набора для автоматического восстановления системы после аварии (*Automated System Recovery*).

- **Архивирование и восстановление состояния системы**

Для создания резервной копии состояния системы необходимо в утилите резервного копирования *ntbackup* при создании задания на архивирования отметить галочкой пункт *System State*:





При этом будут архивироваться следующие данные:

- системный реестр;
- база данных зарегистрированных классов объектов (*Class Registration*);
- системные загрузочные файлы;
- база данных служб сертификатов (только на серверах, на которых установлена служба сертификатов);
- база данных *Active Directory* и папка *SYSVOL* (на контроллерах доменов).

Для архивирования состояния системы, а также для последующего восстановления, обязательно нужны права администратора данного компьютера. Восстановление *Active Directory* необходимо выполнять только при загрузке системы в режиме восстановления служб каталогов (запуск меню выбора режимы загрузки операционной системы выбираются в начальный момент загрузки нажатием клавиши F8).

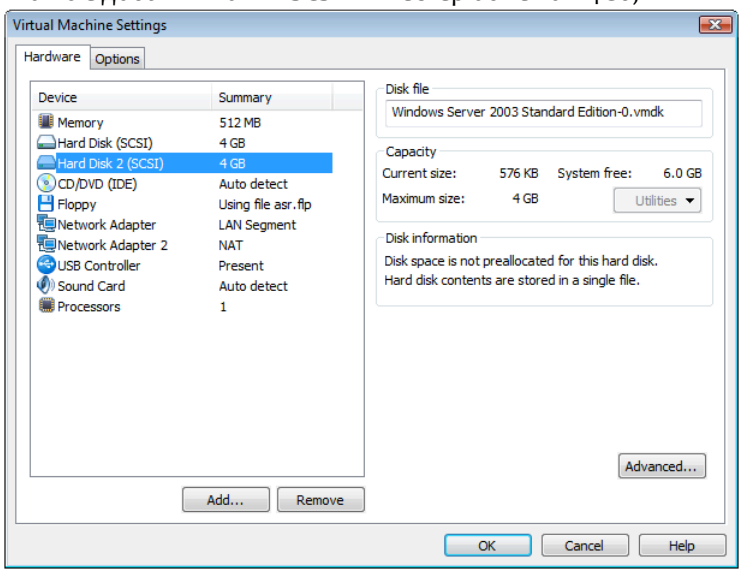
- **Автоматическое аварийное восстановление системы**

В отличие от резервного копирования состояния системы, при котором сохраняется только часть файлов операционной системы, резервное копирования для автоматического аварийного восстановления системы (*ASR, Automated System Recover*) архивирует больший объем информации — практически весь том, на котором установлена операционная система. И процедура восстановления системы становится более сложной.

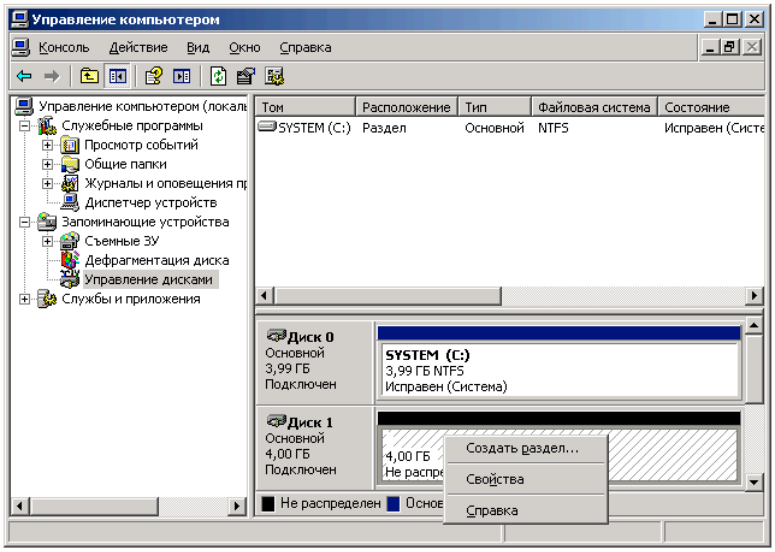
- **Создание ASR-копии**

На данном этапе потребуется носитель для создания резервной копии системного тома (порядка нескольких гигабайт), причем в случае восстановления системы этот носитель должен быть доступен мастеру установки операционной системы (т.е. это либо ленточный накопитель с драйверами для контроллера и накопителя, либо дисковый накопитель с соответствующими драйверами), а также чистая отформатированная дискета для сохранения информации о конфигурации резервной копии.

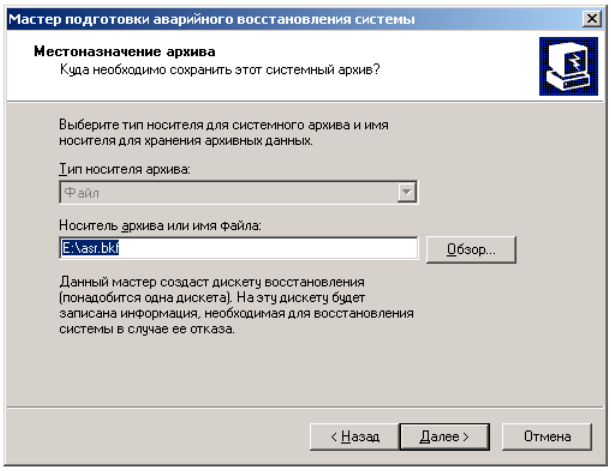
1. Выберем вариант хранения данных на дополнительном дисковом накопителе. Для этого выполним следующие действия:
   - Завершим работу нашего сервера;
   - В настройках данной ОС добавим новый SCSI-винчестер объемом 4Gb;



   - Запустим ОС.
   - Нажмем правой клавишей мыши на «Мой компьютер» и вызываем «Управление»;
   - В управлении дисками инициализируем новый диск;
   - Создаем на нем основной NTFS раздел по всему объему диска.

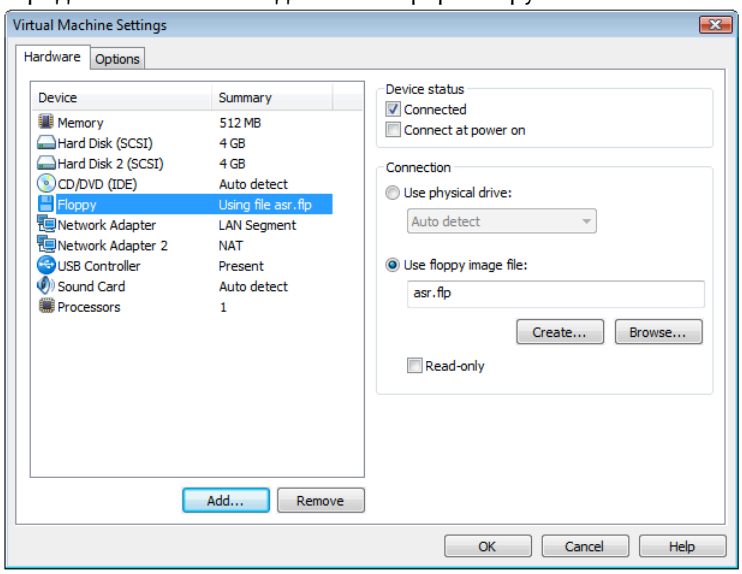


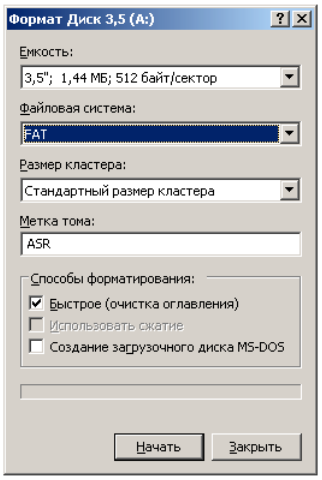
2. Запустим утилиту резервного копирования *ntbackup*.
3. Запустим «Мастер аварийного восстановления системы».
4. Укажем путь для сохранения архива.



5. Нажмем кнопку «Готово». Утилита резервного копирования начнет создание резервной ASR-копии, в нужный момент будет сделан запрос вставить чистую дискету.

Работа с дисководом в WMware имеет определенную специфику. Будем использовать виртуальную дискету. Для этого в свойствах ОС сервера в WMware выберем дискету, выберем «Использовать образ дискеты» и нажмем «Создать». Перед использованием дискеты отформатируйте ее.





После записи конфигурации резервной копии утилита попросит пометить дискету соответствующей информацией (название резервной копии и дата создания).

- **Восстановление системы с помощью ASR-копии**

1. Подготовим все необходимое для аварийного восстановления системы: установочный CD с дистрибутивом операционной системы, носитель с резервной копией, дискету с конфигурацией ASR-копии.

2. Запустим процесс установки операционной системы с загрузочного компакт-диска для этого в BIOSe виртуальной машины сервера установим загрузку с CD;

3. На первой странице мастера установки системы (после появления синего экрана) нажать клавишу F2 для запуска процесса аварийного восстановления.

4. Далее мастер установки системы выполнит новую установку системы с форматированием системного тома.

5. После выполнения установки операционной системы автоматически запустится утилита резервного копирования, и система попросит вас указать путь к резервной копии для аварийного восстановления и вставить дискету с конфигурацией ASR-копии. Будет выполнено восстановление системы из аварийной резервной копии.

6. После завершения процесса восстановления будет воссоздан работоспособный сервер в той конфигурации, которая была до аварии (при условии, конечно, что, кроме самой системы, будут также восстановлены и данные, необходимые для работы сервера).

7. В BIOSe виртуальной машины сервера установим загрузку с HDD;

Корпорация Microsoft рекомендует использовать данный метод восстановления для серверов, выполняющих особые функции, которые трудно восстановить простой переустановкой и восстановлением данных. Если сервер не исполняет какие-либо особые роли, то Microsoft рекомендует на таких серверах архивировать только данные, а в случае аварии заново переустановить сервер, снова включить его в домен и восстановить данные из резервных копий.

Служба резервного копирования Microsoft Windows Server 2008.

Кратко об утилите архивирования

Сначала надо установить утилиту резервного копирования, потому что по умолчанию она не устанавливается. Откройте в диспетчере сервера (Server Manager) Мастер добавления компонентов (Add Features Wizard) и добавьте компонент «Возможности системы архивации данных Windows Server» (Windows Server Backup Features) (**рис. 1**). Нам нужен подкомпонент, позволяющий использовать команды командной строки, что позволяет использовать Windows PowerShell. Для установки этого подкомпонента можно также использовать средства командной строки так: C:\ servermanagercmd –install backup-features.

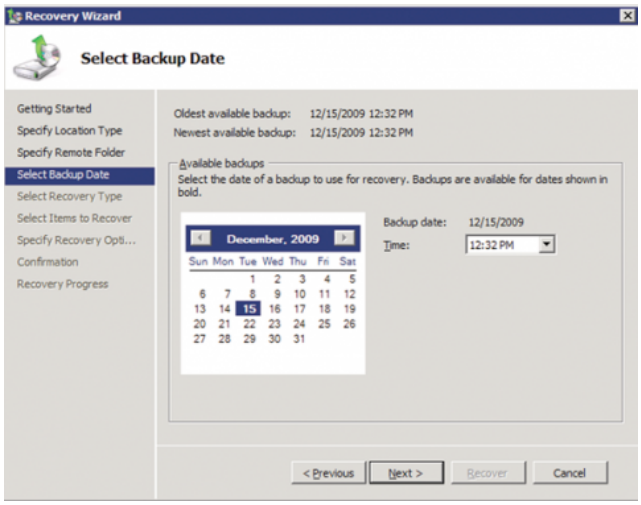


Рис. 1 **Использование мастера добавления компонентов для установки системы архивации данных Windows Server и средств командной строки.**

Далее следует указать место, где будут храниться резервные копии. Файлы можно хранить на общем сетевом томе, на локальном томе или выделенном диске. Нельзя копировать данные на пленку, но ввиду широко распространения недорогих подключаемых USB-устройств сейчас это уже не выглядит как серьезный недостаток. Однако есть ряд обстоятельств, которые надо учесть.

Резервное копирование Windows создает существенную дополнительную нагрузку ввиду необходимости создания дополнительных индексов, каталогов и других вспомогательных файлов. Это уже не простое создание ZIP-файла. Не надо рассчитывать, что резервная копия файла общим объемом 100 Кб займет столько же места на диске — ее размер будет существенно больше.

При копировании на сетевую папку надо внимательно отнестись к уровню доступа к файлам, чтобы обеспечить целостность и защиту резервных копий. Также надо иметь в виду, что при копировании в общую сетевую папку, предыдущая резервная копия перезаписывается. Самое простое решение — создавать подпапку для каждой резервной копии. Та же история с размещением резервных копий на локальном томе.

Одно из преимуществ использования сетевой папки или тома состоит в том, что утилита архивации Windows создаст файл с расширением .vhd, содержащий все копируемые файлы. При определении места хранения резервных копий утилита архивации Windows создаст папку верхнего уровня по имени WindowsImageBackup. В этой папке создаются подпапки для каждого компьютера. Версии резервных копий различаются по времени; вот пример имени папки:«Backup

2009-12-14 172606».В этой папке хранятся архивы и VHD- файл. Этот VHD- файл можно подключить в Windows 7 или Windows Server 2008 R2. В зависимости от вида резервной копии и требований по архивации этот файл можно переместить на диск долгосрочного хранения или на DVD-диск.

Самый простой и быстрый вариант — выделенный подключенный диск. Он может внутренним или внешним с интерфейсом USB или FireWire. Microsoft рекомендует, чтобы на диске было в 2,5 раз больше свободного пространства, чем необходимо для создания архива всех архивируемых данных. Диск надо отформатировать и скрыть от обычных инструментальных средств управления — он должен быть доступен только в панели Управление дисками (Disk Management). Поддерживаются диски объемом до 2 Тб.

Создание задания резервного копирования

Утилита архивирования Windows задумана как универсальный инструмент защиты сервера. Можно создать регулярное задание архивирования файлов и состояния системы или обеспечить возможность восстановления целого сервера «с нуля». Microsoft предполагает, что для этой цели создается одно задание. Я предполагаю, что вы используете возможности утилиты архивирования Windows из-за ограниченного бюджета и хотите получить от нее максимально возможную защиту при существующих ограничениях.

Установив утилиту архивирования Windows, в Диспетчере сервера разверните узел «Хранилище» (Storage) и выберите «Архивирование сервера Windows» (Windows Server Backup). В панели Действие (Action), выберите «Задание архивирования» (Backup Schedule) — откроется Мастер архивации по расписанию (Backup Schedule Wizard). На первой странице мастера щелкните Далее (Next).

На второй странице мастера определите тип архива. Выберите полную резервную копию сервера. Вы можете выбрать пользовательскую резервную копию и выбрать архивируемые элементы, например определенные файлы и состояние системы. Как делать быстрое резервное копирование файлов, я покажу чуть позже, а пока сделаем полную копию сервера.

На третьей странице задается время выполнения задания. В большинстве случаев одного резервного копирования достаточно, но можно запускать его чаще раза в день, например резервное копирование критически важных файлов.

На четвертой странице определите, где хранить резервные копии. Microsoft рекомендует использовать выделенный жесткий диск. Имейте в виду, что диск будет переформатирован и недоступен для каких-либо других операций. Можно также использовать локальный или сетевой том. Внимательно ознакомьтесь с предупреждениями и информацией об ограничениях — наверняка вы увидите предупреждение, что выбранный диск будет переформатирован.

Если все диски не видны, щелкните кнопку «Все доступные диски» (Show All Available Disks), чтобы обновить список. Утилита выдаст предупреждение, если вы выберете новый диск. Задав диск, переходят к проверке параметров архивирования. Если что-то не так, используйте кнопку Назад (Previous), чтобы вернуться и устранить ошибку. Если все правильно, должно открыться окно сводки. На следующий день проверьте результаты выполнения задания в узле утилиты архивирования Windows на предмет сообщений об ошибках.

Вы можете также использовать утилиту архивирования Windows для одноразового создания резервной копии. Выберите вариант «Однократная архивация» (Backup Once) в панели Действие (Actions). Вы можете использовать те же параметры, что и у существующего задания, или задать совершенно другие. Если выбрать второй вариант, мастер перезапустится, предоставив возможность ввести новые параметры. Например, скопировать файлы на сетевой том. Помните, что любые существующие резервные копии в той же папке будут перезаписаны. Резервное копирование начинается немедленно. Если же это отдельное задание резервного копирования, которое нужно выполнять часто, рекомендуем создать сценарий командной строки или Windows PowerShell. Я расскажу об этой процедуре позже.

Восстановление данных

Для отслеживания версий утилита архивирования Windows использует метки времени. При выборе команды Восстановление (Recover) запускается мастер, инструкции которого практически самоочевидны. Выберите резервную копию. Мастер восстановления предоставит список всех доступных резервных копий . Выберите нужный архив. В зависимости от типа резервного копирования может быт только один вариант.

Далее указывают данные, которые надо восстановить. Если выбрать «Файлы и папки» (Files and Folders), потребуется указать нужные файлы. К сожалению, выбор файлов из нескольких каталогов практически невозможен. Восстановить все файлы или выбранные файлы одного каталога намного проще. Не забывайте об этом, создавая задание резервного копирования.

Восстанавливая файлы, надо указать целевую папку:это может быть та же папка, которую архивировали, или любая другая. Вы также можете определить, что должно произойти с восстанавливаем файлом, если он уже существует: создать еще одну копию, чтобы были доступны обе копии, перезаписать существующий файл или не выполнять восстановление. Процесс восстановления начинается немедленно.

Использование WBADMIN.EXE

Если установить средства архивирования из командной строки, у вас появляются еще несколько вариантов. Откройте окно командной строки и ознакомьтесь со справкой WBADMIN.EXE. Эту утилиту можно использовать для создания запланированного задания архивирования, но я все-таки думаю, что для выполнения этой задачи графический интерфейс намного удобнее. WBADMIN.EXE полезнее для создания одноразовых заданий резервного копирования. Выполните следующую команду, чтобы увидеть информацию о синтаксисе:

C:\> wbadmin start backup /?

Здесь недостаточно места для рассказа о всех вариантах, но я покажу, как можно использовать эту утилиту для периодического копирования файлов на сетевой том:

```
@echo off ::Demo-Backup.bat ::demonstration script using WBADMIN.EXE on a Windows Server 2008 R2 Server  rem backup share UNC set backupshare=\\mycompany-dc01\backup rem files and folders to include set include=c:\scripts,c:\files  rem define date time variables for building the folder name set m=%date:~4,2% set d=%date:~7,2% set y=%date:~10,4% set h=%time:~0,2% set min=%time:~3,2% set sec=%time:~6,2%  rem defining a new folder like \\mycompany-dc01\backup\RESEARCHDC\12152009_132532 set newfolder=%backupshare%\%computername%\%m%%d%%y%_%h%%min%%sec% echo Creating %newfolder%  mkdir %newfolder%  rem run the backup echo Backing up %include% to %newfolder% wbadmin start backup -backuptarget:%newfolder% -include:%include% -quiet rem Clear variables set backupshare= set include= set m= set d= set y= set h= set min= set sec= set newfolder=
```

Я не хочу перезаписывать существующие резервные копии, поэтому я создаю новую папку с именем компьютера, а имя файла содержит штамп времени. В данном пакетном файле есть весь код, необходимый для решения задачи. Основная функция сценария вызывает WBADMIN.EXE для создания резервной копии в заданном месте. При модификации этого сценария не забывайте поглядывать в справку по синтаксису команды. В этом сценарии мне нравится возможность создавать собственное задание, используя планировщик задач. Мастер архивации позволяет создать только одно задание, а используя WBADMIN.EXE, а могу создать их сколько угодно.Я могу также использовать этот инструмент для создания резервных копий состояния системы.

Чтобы узнать, какие задания резервного копирования были выполнены, выполните команду: C:\> wbadmin get versions.

Особое внимание надо обращать на идентификатор версии, так как он необходим для восстановления файлов средствами WBADMIN (впрочем это же можно делать средствами мастера восстановления).

Резервное копирование средствами Windows PowerShell

Другой способ задействовать командную строку состоит в использовании командлетов PowerShell утилиты архивирования Windows. Чтобы получить к ним доступ, надо загрузить оснастку архивирования Windows:

PS C:\> add-pssnapin Windows.ServerBackup

Чтобы увидеть список доступных командлетов, выполните команду:

PS C:\> get-command -pssnapin windows.serverbackup

К сожалению, создание задания резервного копирования — многошаговый процесс. Хотя нужные команды можно вводить в окно последовательно вручную, я предпочитаю писать сценарии. Вот PowerShell-версия моего исходного пакетного файла:

```
#requires -version 2.0 #requires -pssnapin Windows.ServerBackup  #Demo-WBBackup.ps1 $policy = New-WBPolicy $files=new-WBFileSpec c:\scripts,c:\files Add-wbFileSpec -policy $policy -filespec $files $backdir=("\\mycompany-dc01\backup\{0}\{1:MMddyyyy_hhmmss}" -f $env:computername,(get-date))  write-host
```

```
"Creating $backdir" -foregroundcolor Green mkdir $backdir | out-null  $backupLocation
= New-WBBackupTarget -network $backdir  Add-WBBackupTarget -Policy $policy -Target
$backupLocation  write-host "Backing up $files to $backdir" -foregroundcolor Green
$policy Start-WBBackup -Policy $policy
```

Идеология командлетов Windows PowerShell основана на создании и выполнении политик. Политика содержит включаемые или исключаемые файлы или тома, место, куда надо копировать файлы, а также несколько других параметров. Можно также создавать задания восстановления состояния системы и восстановления целого сервера «с нуля». В своем примере я просто копирую несколько каталогов. Для резервного копирования задействуется командлет Start-WBBackup.

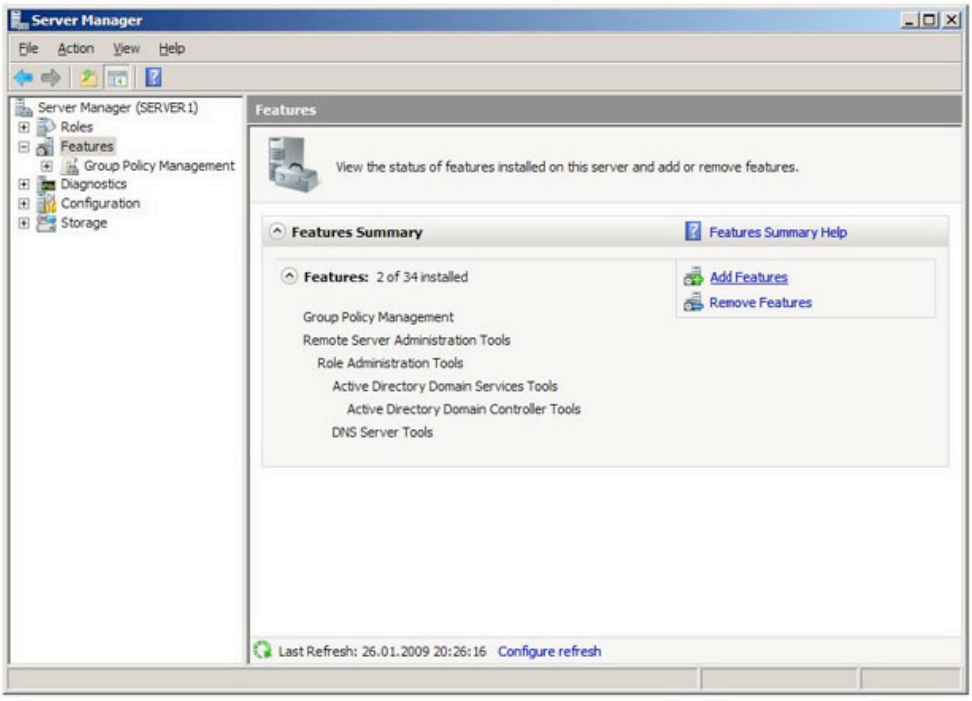
При более близком изучении списка командлетов утилиты архивирования Windows заметен один явный пробел: нет никаких командлетов для восстановления данных. Я полагаю, что эту операцию не нужно автоматизировать, хотя это и можно сделать с помощью WBADMIN.EXE. Возможно такие командлеты будут добавлены позже, а пока для восстановления файлов можно пользоваться мастером восстановления или WBADMIN.EXE.

С точки зрения управления рисками, важность процедуры резервного копирования очень высока. В тех случаях, когда реализация угрозы приводит к изменению или удалению данных, повреждению программных компонент системы, резервное копирование позволяет снизить причиненный ущерб и значительно ускорить восстановление системы.

При разработке политики резервного копирования нужно определить, как минимум, следующие параметры:

- частоту выполнения резервных копий;
- порядок восстановления данных из резервных копий;
- объем носителей информации, выделяемых для хранения резервных копий;
- количество хранимых копий;
- вопросы обеспечения безопасности носителей резервных копий.

Утилиты резервного копирования Windows Server 2008 существенно отличаются от того, что было в Windows Server 2003 (где эти задачи решались с помощью утилиты ntbackup). Чтобы их использовать, для начала требуется их установить (по умолчанию, они не устанавливаются). Делается это с помощью оснастки **Server Manager**, где надо выбрать пункт **Add Feature** в разделе **Features** (рис. 10.1) и в появившемся списке выбрать пункт **Windows Server Backup Features** (рис. 10.2.).



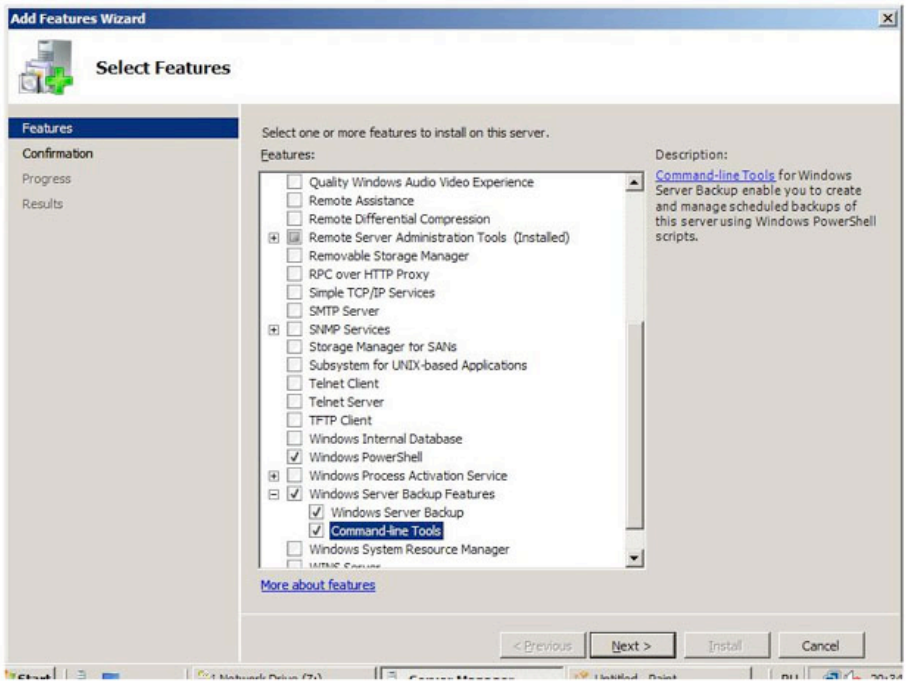
увеличить изображение
Рис. 10.1. Оснастка Server Manager позволяет добавить компоненты

Как видно на рис. 10.2, предлагается выбрать следующие опции:

- Windows Server Backup;

- Command-line tools (утилиты командной строки).

Установка последних, позволяет управлять резервным копированием с помощью сценариев и требует установки Windows PowerShell. Но для выполнения лабораторной будет достаточно установить только Windows Server Backup.



увеличить изображение
Рис. 10.2. Добавляем утилиты администрирования

После установки, в меню **Administrative Tools** становится доступной оснастка **Windows Server Backup**. С ее помощью можно проводить резервное копирование данных на локальном или удаленном компьютере (если это разрешено настройками).

Рассмотрим, как это происходит. Запустим утилиту. Резервное копирование может проводить пользователь, состоящий в группе **Administrators** (Администраторы) или **Backup Operators** (Операторы архива). При этом, у членов группы **Backup Operators** при запуске оснастки **Windows Server Backup** будет дополнительно запрашиваться пароль (в окне **User Account Control**), т.к. эти операции относятся к разряду потенциально опасных.

В окне оснастки в списке доступных действий (**Actions**), расположенном в правой части экрана, выберем опцию **Backup Once …** (т.е. однократная архивация). Запустившийся мастер резервного копирования предложит выбор между настройками для уже запланированного копирования (**The same options that you used in the Backup Schedule Wizard for scheduled backups**) и новыми (**Different options**). Нужно выбрать второй вариант (если, как в нашем примере, утилита ранее не использовалась, то первый пункт списка будет неактивен).

Следующее окно мастера позволяет выбрать, производить ли полное резервное копирование или копирование отдельных разделов (рис. 10.3). Здесь проявляется первое отличие новых инструментов - резервное копирование отдельных папок и файлов производить нельзя, только логический диск целиком.

Хотелось бы также обратить внимание на надпись в нижней части экрана, там дается ссылка на раздел справки, описывающий выполнение с помощью утилиты командной строки резервного копирования только состояния системы (**System State**).

Выберем вариант **Custom**.

Тогда на следующем экране появится список дисков (рис. 10.4). Устанавливая или снимая отметки, можно указать, данные с каких дисков помещаются в резервную копию. Опция **Enable System Recovery** включает в архив разделы, где находятся компоненты операционной системы и файлы необходимые для загрузки (т.е. отметку напротив этих разделов будет не снять).

Предположим, нам нужно сделать резервную копию диска E:, на котором находятся пользовательские данные. Тогда отметки устанавливаем так, как это сделано на рис. 10.4 и переходим к следующей стадии, на которой нужно

определить, куда будет производиться копирование. Это может быть локальный диск (жесткий диск, пишущий DVD-привод и т.д.) или сетевая папка. Надо учитывать, что архивная копия не может сохраняться на диск, входящий в перечень архивируемых. Также нельзя сохранить архив на диск, где хранятся файлы операционной системы

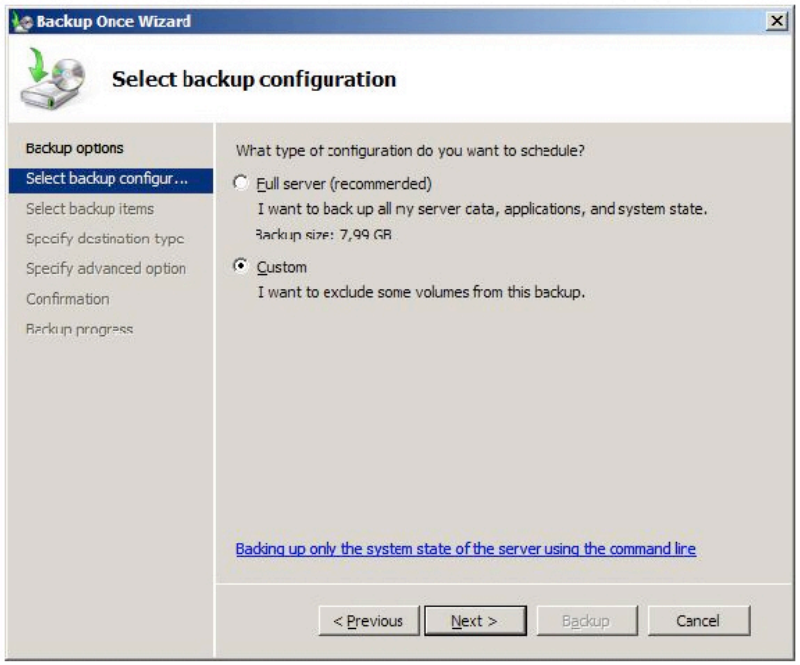


Рис. 10.3. Выбор между полным резервным копированием и копированием отдельных дисков

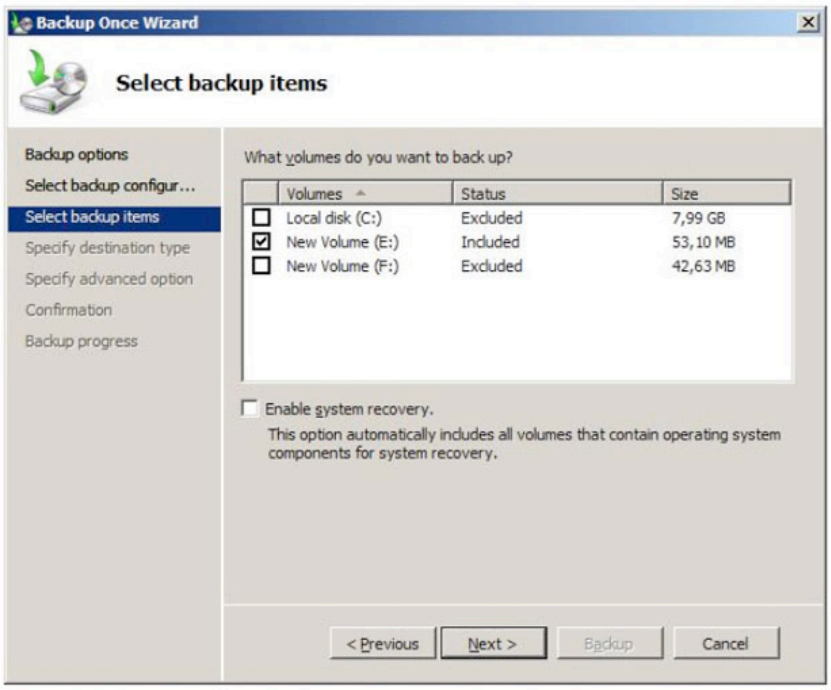


Рис. 10.4. Выбор дисков для резервного копирования

Учитывая все вышеизложенное, в рассматриваемом примере можно сделать резервную копию диска E: на диск F:, в сетевую папку или на DVD-диск. Выберем первый вариант, что и укажем в следующем окне мастера. После чего будет предложено выбрать тип резервного копирования (рис. 10.5).

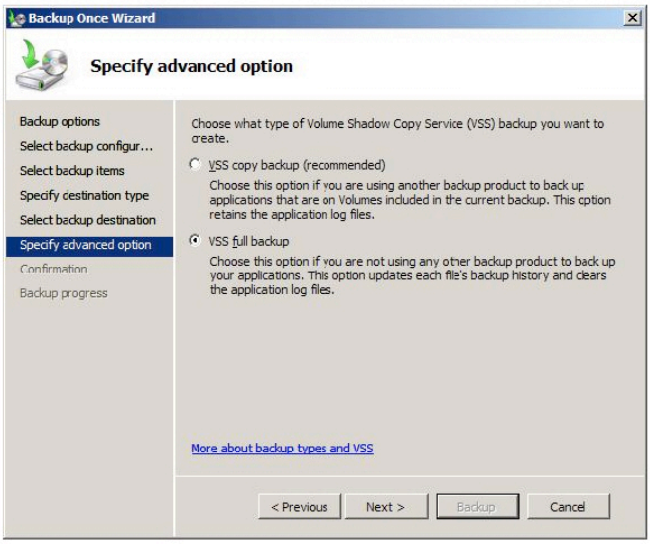


Рис. 10.5. Выбор типа копирования

Служба Volume Shadow Copy Service (VSS) может при резервном копировании отмечать файлы, как помещенные в архив, или не делать это. Если кроме средств Windows Server 2008 используются и другие продукты для резервного копирования, рекомендуется выбрать вариант **VSS copy backup**. Если такого нет, можно смело выбирать вариант **VSS full backup**.

В следующем окне мастера будет запрошено подтверждение и, если оно получено, запустится резервное копирование.

В результате, в нашем примере на диске F: появится каталог **WindowsImageBackup**, в нем будет создан подкаталог, названный по имени архивируемого сервера, куда и попадет копия.

Вывод. Сетевой администратор (ИТ-руководство компании) должны уделять вопросам резервного копирования самое пристальное внимание, т.к. от грамотно построенной и надежно работающей системы резервного копирования зависит, насколько быстро и удачно будет произведено восстановление информации, поврежденной в результате действий персонала, аппаратных сбоев, вирусных атак и прочих инцидентов.

Задание

1. На учебном сервере (или виртуальной машине) выберите раздел для резервного копирования.
2. С учетом рассмотренных ограничений и объема копируемого раздела, выберите место для размещения копии. Определите, от имени какой учетной записи будет проводиться эта операция.
3. Выполните однократное резервное копирование выбранного раздела.

Контрольные вопросы:

1. Какие причины резервирования данных?
2. Какие существуют типы резервного копирования?
3. Какие преимущества дает механизм теневых копий?
4. Какие типы резервного копирования Вы знаете? В чем их особенности?
5. Кто планирует какие данные нужно резервировать?
6. Какие недостатки имеет архивирование, проделанное в данной лабораторной работе?
7. Какие данные необходимо резервировать?