восстановление MS Server 2003 после тяжелых ранений

крис касперски, ака мыщъх, a.k.a nezumi, a.k.a. souriz, a.k.a. elraton, no-email

MS Server 2003 – достаточно надежная и неприхотливая система, средняя наработка на отказ которой составляет несколько лет. для борьбы с падениями народ вовсю использует Norton Ghost, Acronis True Image и другие сторонние утилиты, стоящие не мерянных денег и плохо работающие (или совсем не работающие) со SCSI-дискам/RAID-массивами, но про штатный MS BackUp никто и слушать не хочет — все сразу начинают махать руками и гнать волну. плох же тот мастер, кто свой инструмент не знает! мыщъх использует MS BackUp уже более семи лет и со всей ответственностью заявляет, что это отличное средство восстановления системы, обладающее огромным скрытым потенциалом, о котором мыщъх сейчас и расскажет

введение

Почему "падает" MS Server 2003? Причины на самом деле очень различны и если попытаться огласить весь список, то получится здоровенный талмуд, поэтому, мы перечислим лишь наиболее значимые из них:

- установка "кривого" программного обеспечения (пакетов обновлений, прикладных приложений, драйверов, etc), вызывающее конфликты разной степени тяжести и/или ведущее к разрушению критических структур данных;
- сбои питания и/или дефекты оборудования, нарушающие целостность системного кода/данных;
- вирусные эпидемии и хакерские атаки, завершающиеся внедрением нестабильно работающего root-kit'a;
- ошибки оператора, удалившего жизненно важные системные файлы, отключившего базовые службы или сделавшего иную глупость;

Так же приходится сталкиваться с физическими отказами жесткого диска, контроллера RAID-массива, разрушением главной загрузочной записи, boot-сектора и другими катастрофами планетарного масштаба, требующих для восстановления данных не только соответствующих навыков, но, в ряде случаев, и весьма дорогостоящего оборудования.

К счастью, такие происшествия случаются нечасто, и в наших рассуждениях мы будем исходить из того, что жесткий диск (RAID-массив) на аппаратном уровне функционирует исправно, файловая система цела (или, на худой конец, может быть вылечена штатной утилитой chkdsk).

Пострадала лишь сама операционная система, причем тяжесть разрушений колеблется от нестабильной работы до полного отказа загружаться. Более сложные случае восстановления мы не рассматриваем, отсылая читателя к серии статей "восстановление данных на NTFS разделах" и книгам "техника восстановления данных"/"data recovery tips and solutions", электронные копии которых лежат на мыщъхином сервере: http://nezumi.org.ru/recover.zip, http://nezumi.org.ru/ recover-full-rus.zip, http://nezumi.org.ru/recover-full-eng.zip. Естественно, совершенно бесплатно.

Хочется еще раз напомнить читателю, что залогом сохранности данных была и остается резервная копия, о технике создания которой мы и будем говорить. При нынешних ценах на сменные носители отсутствие резервной копии объясняется лишь полной безответственностью системного администратора или неумением автоматизировать процесс резервирования в условиях интенсивного изменения больших объемов данных, рассосредоточенных по десяткам (а то и сотням компьютеров!). Но объяснение — это еще не оправдание!!! Приговором (в случае разрушения) становится кропотливая работа ручного восстановления "осколков" данных, когда файлы приходится собирать буквально по кусочкам. И стоит это работа намного больше носителей для резервного копирования. Добавьте сюда еще простой организации на время восстановления и вы поймете, почему в настоящей статье мы будем говорить _только_ об утилите MS BackUp, оставив остальные способы восстановления за кадром.

создание резервной копии

Набираем в командной строке "ntbackup.exe" (именно "nt", а не "ms") и дожидаемся запуска (поклонники графических сред и мыши могут воспользоваться другим путем: "My Computer → Any Disk → Properties → Tools → Backup Now").

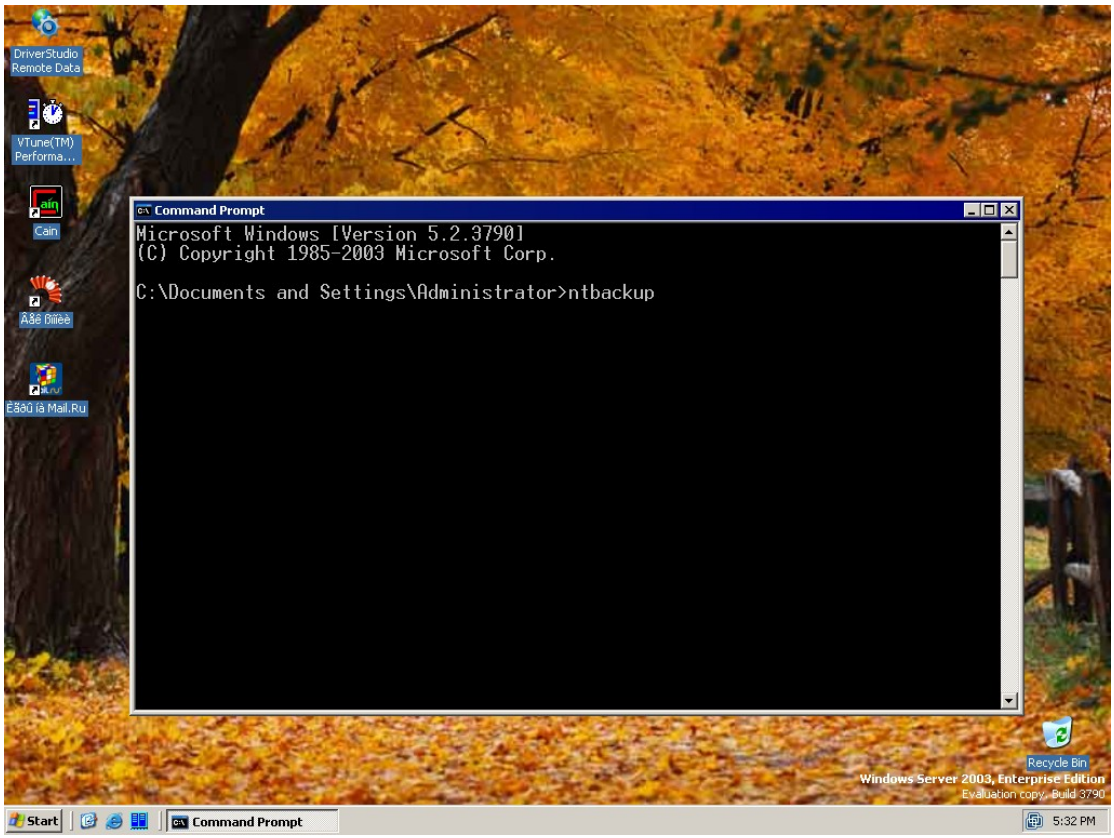

Рисунок 1 запуск MS BackUp из командной строки

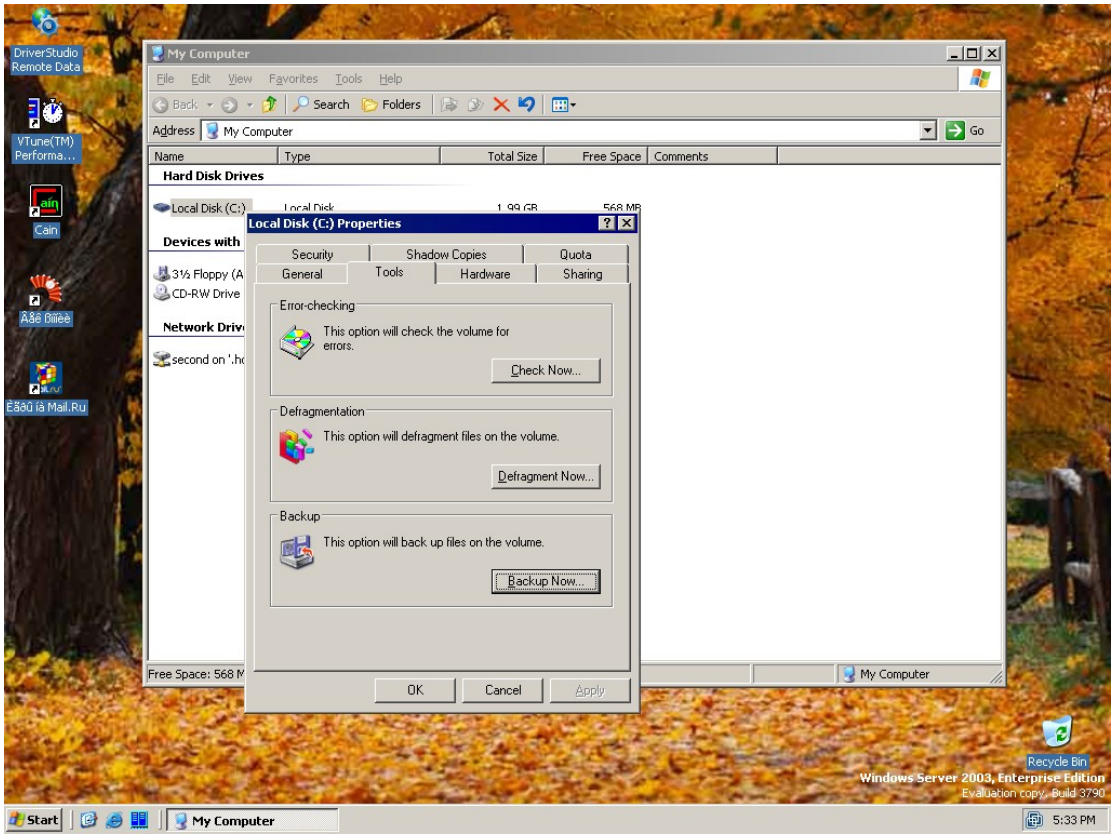

Рисунок 2 запуск MS BackUp через проводника Windows

Главное окно приложения с большими прямоугольными кнопками, вызывающими различных мастеров (см. рис. 3), сразу пропустим (мы же не пользователи какие-нибудь, а самые настоящие администраторы!), и перейдем непосредственно к вкладке "Backup".

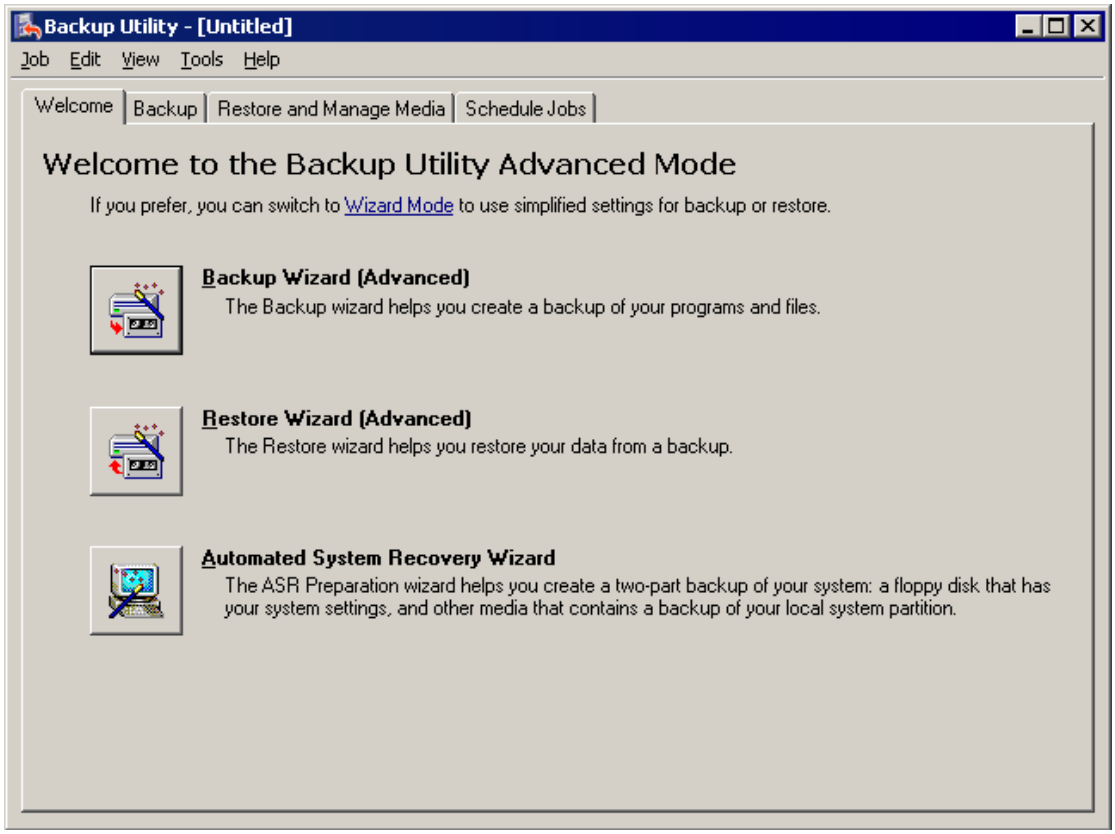

Рисунок 3 главное окно программы с кнопками различных мастеров

Здесь, во вкладке "Backup" (см. рис. 4), мы отмечаем галочкой пункт "System State" (состояние системы) форсирующих архивирование следующих компонентов (перечисленных в колонке справа): загрузочные файлы, реестр, и классы COM+. К сожалению, мы не можем влиять на выбор компонентов, что есть большая вселенская несправедливость, поскольку в подавляющем большинстве случаев система дохнет из-за разрушения реестра или классов.

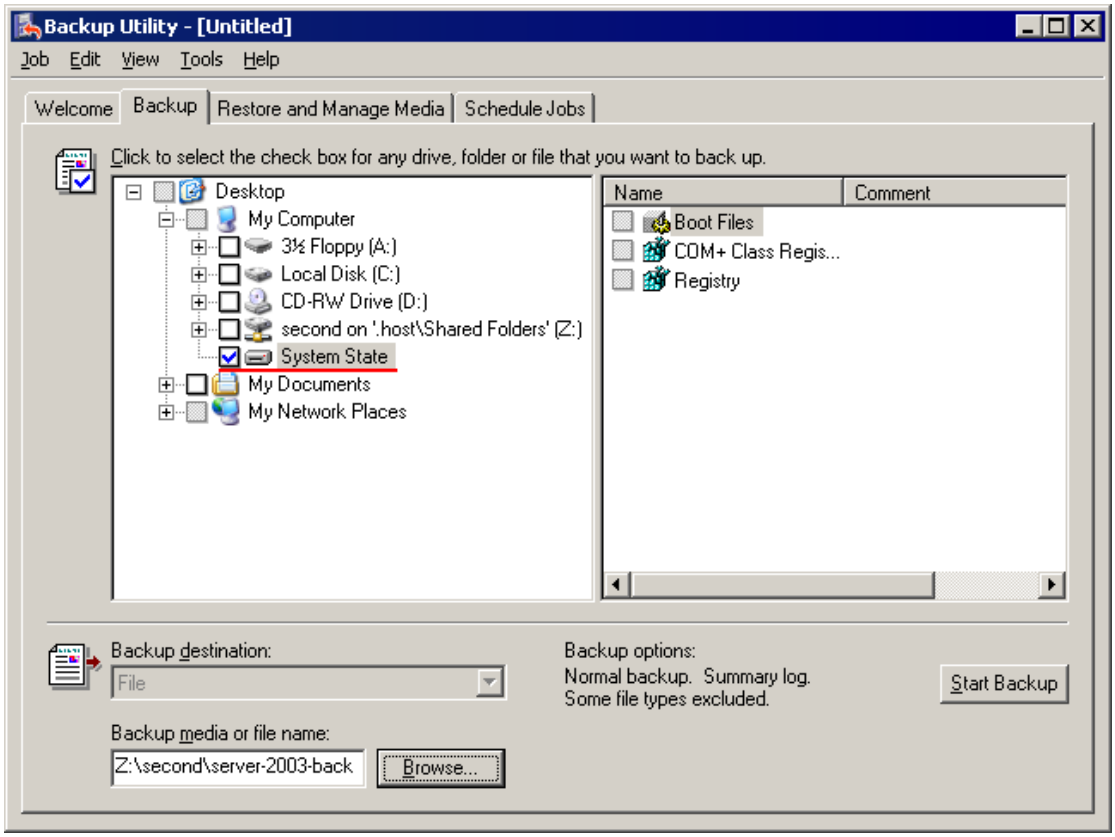

Рисунок 4 вкладка Backup, позволяющая среди прочего сохранять состояние системы

Указываем путь к файлу архива в строке "Backup media of file name" и нажимаем "Start Backup", после чего нас запросят описание и метку архива (backup description/label) и способ его создания — append (дозапись в конец) или replace (замещение старых данных). По своему личном опыту мыщъх рекомендует не класть все яйца в одну корзину, то всегда создавать архивный файл заново, отказавшись от идеи дозавписи в его конец, поскольку это чревато целым рядом различных проблем (см. рис. 5, слева).

Нажав кнопу "Advanced" (дополнительные опции) мы можем выбрать тип архива (см. рис. 5, справа): normal (полная архивация, со снятием атрибута архивный), copy (полная архивация без снятия атрибута архивный), incremental (архивирование только измененных или вновь созданных файлов), differential (тоже самое, что incremental, только без снятия атрибута архивный), daily (архивирование файлов, измененных в течении дня). Последние три типа архивов требуют для восстановления normal/copy архивов и всей цепочки incremental/differential/daily архивов, что часто приводит к путанице и снижает вероятность успешного восстановления, особенно если хотя бы один из архивов поврежден, так что мыщъх рекомендует всегда выбирать тип "normal", несмотря на то, что он требует больше времени, чем последние три.

Галочка "Verify data after backup" (проверка целостности данных после архивирования) при резервировании на жесткий диск бессмысленна и поэтому ее лучше не взводить, а вот "Automatically backup System Protected Files with the System State" ("Автоматически архивировать Защищенные Системные Файлы вместе с состоянием системы") лучше оставить взведенной по умолчанию.

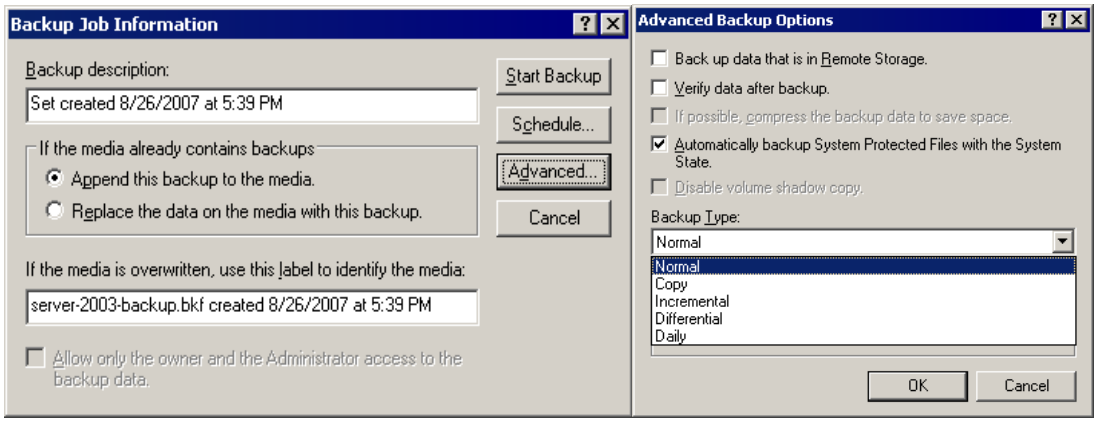

Рисунок 5 диалоговое окно с меткой/описания архива и способом его (пере)записи (слева) и диалоговое окно "тонких" настроек, задающее тип архива (справа)

Наконец, после нажатия на кнопку "Start Backup" начинается процесс архивации (см. рис. 6), занимающий (в зависимости от быстродействия системы) от нескольких минут до получала. На выходе мы получаем bkf-файл с размером порядка 400 Мегабайт (точный размер зависит от версии системы, количества установленных заплаток, драйверов и приложений), но в своей практике мыщъх еще не сталкивался с тем, чтобы bkf-файл (типа "replace") не влезал бы на один CD-R/RW диск, не говоря уже о DVD-R/RW. Хранить на жестком диске архив небезопасно, впрочем, как показывает, практика, оптические носители сыплются еще чаще, так что несколько копий никому не помешают.

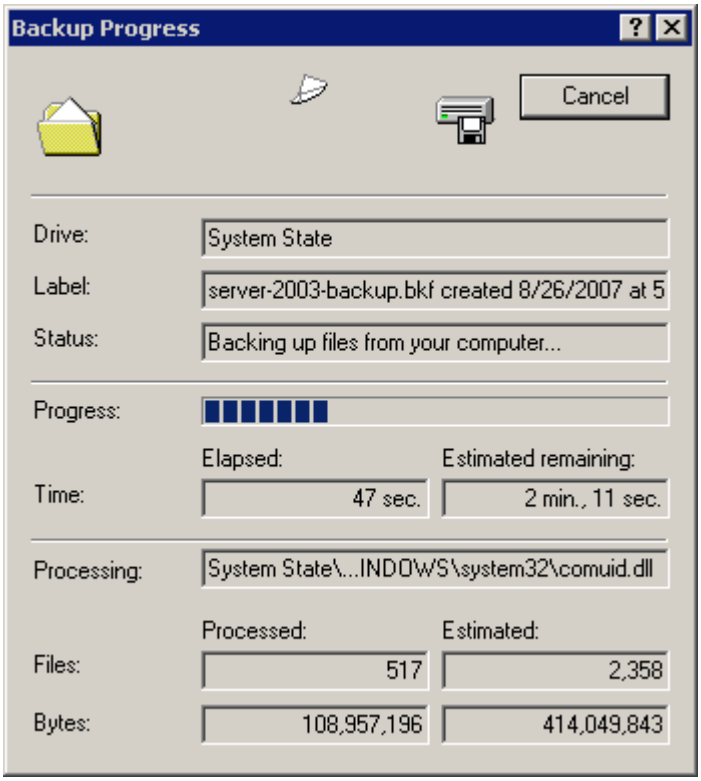

Рисунок 6 процедура сохранения состояния системы в архивный bkf-файл

ОК, мы имеет архив состояния системы и если вдруг Server 2003 начнет вести себя нестабильно, мы всегда сможем выполнить откат. Приложения и драйвера, установленные _после_ создания архива, в большинстве случаев отката не переживут и сдохнут (зависит от того в какие ключи реестра они себя прописывают) и потребуют переустановки, которая в свою очередь не всегда возможна, поскольку после "отката" в системе присутствуют их обломки и как поведет себя инсталлятор совершенно неясно.

Поэтому, вырабатываем следующую стратегию поведения. Создаем архив системы. Устанавливаем новое приложение/драйвер/заплатку. Тестируем сервер в течении некоторого времени (например, недели), если полет нормальный — создаем новый архив системы, а старый удаляем. Если же после установки приложения/драйвера/заплатки появляются глюки, неустранимые деинстяллятором, выполняем принудительный откат через MS BackUp.

Эта бесхитростная схема позволила мыщъху продержать пару серверов и пяток рабочих станций более семи лет без переустановки системы.

>>> врезка что находится внутри системного архива

Чтобы лучше понять возможности (и ограничения!) MS Backup, необходимо знать какие именно файлы она кладет при сохранении системы, а кладет она туда следующее:

- некоторые ветви реестра, сосредоточенные в файлах: system, software, security, sam, default, ComRegDb.bak, образующие ветвь HKEY_LOCAL_MACHINE (остальные ветви реестра _не_ сохраняются);
- практически все содержимое папок Sytem32 и System (стратегия отбора файлов не совсем понятна, похоже, берутся все жизненно необходимые компоненты плюс некоторые файлы, относящиеся к установленным приложениям сторонних разработчиков);
- некоторые важнейшие файлы и папки из каталога Windows (например, AppPatch, msagent, MICROSOFT.NET, etc);
- отдельные файлы и папки из каталога PROGRAM FILES (например, COMMON FILES, Internet Explorer, Outlook Express, etc);
- содержимое каталога RSA\MachineKeys из папки DOCUMENTS AND SETTINGS\ALL USERS\APPLICATION DATA\ MICROSOFT\CRYPTO, содержащее ключи шифрования (если, конечно, таковые имеются);

Остальные файлы (в том числе и пользовательские учетные записи) _не_ сохраняются, хотя ничего не мешает указать их вручную, проставив соответствующие галочки в напротив папок "DOCUMENTS AND SETTINGS\<Имя пользователя>" или сохранить их вручную, через FAR или другой менеджер файлов.

простые случае восстановления

Система глючит, работает нестабильно, но, все-таки загружается, позволяя нам запустить MS BackUp и выполнить откат к стабильному архиву. Если же Server 2003 зависает или выбрасывает голубой экран на стадии загрузки, попробуйте при запуске нажать <F8> (см. рис. 7) и выбрать "Safe Mode" (или "Safe Mode with Networking", если храните архивы на отдельном сервере, как, например, поступает мыщъх). Так же можно попробовать выбрать пункт "Last Known Good Configuration" (загрузка последней удачной конфигурации).

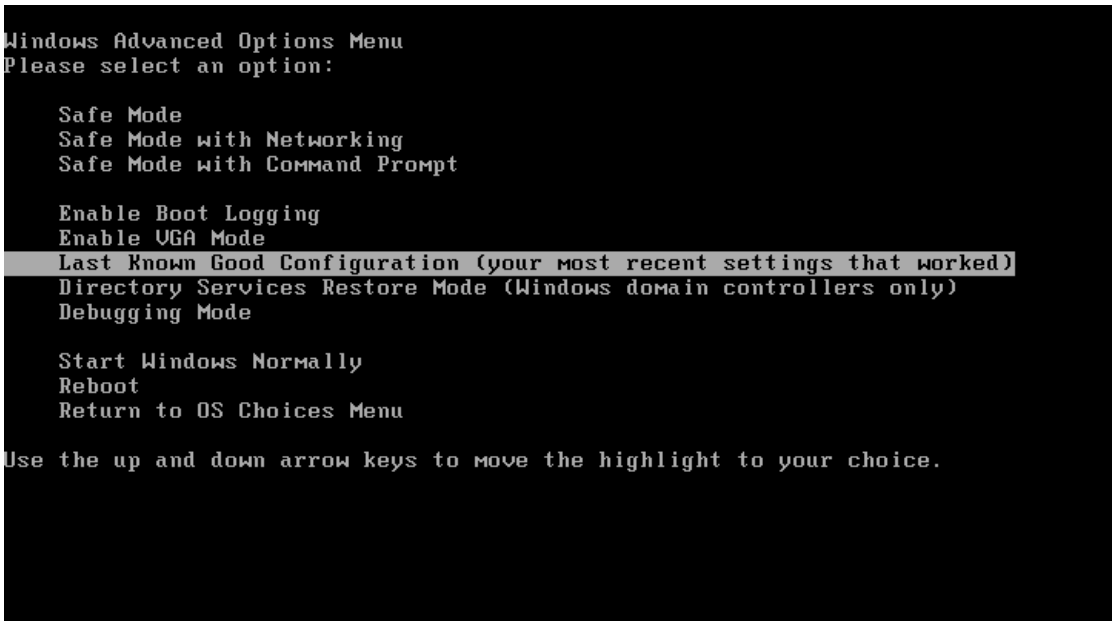

Рисунок 7 диалоговое окно, вызываемые по <F8>, и позволяющее загружать даже практически полностью рухнувшую систему

В общем, крутитесь как хотите, но добейтесь загрузки системы, после чего запускайте "ntbackup" и не мешкая (ведь система может упасть в любой момент) переходите к вкладке "Restore and Manage Media" (Восстановление и Управления Носителями).

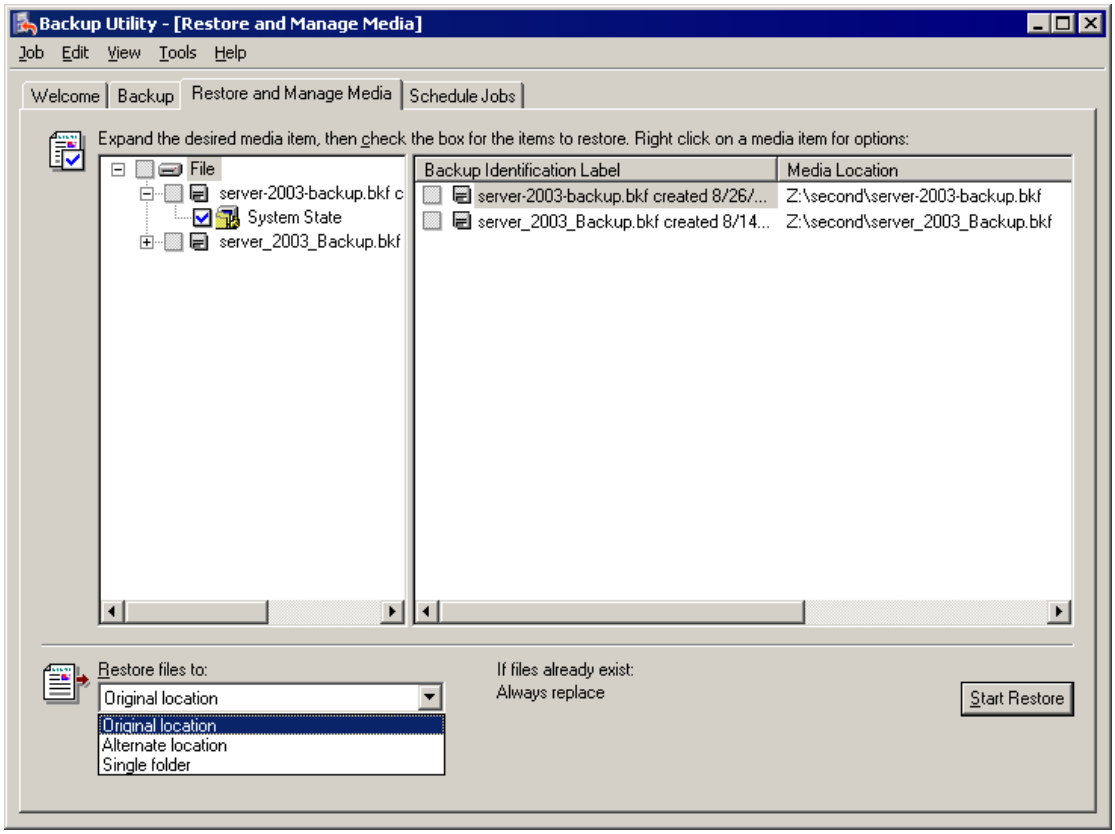

Рисунок 8 восстановление состояние системы из bkf-архива в исходную локацию

Здесь (см. рис. 8) находится перечень всех bkf-архивов с описаниями и метками, которые мы только успели создать. Достаточно распахнуть соответствующую ветвь в левом окне, выбрав самый свежий архив и установить галочку напротив "System State". По умолчанию архив ищется в той же локации, где он был создан, но мы можем изменять путь, нажав кнопку "Browse" и указав, к примеру, лазерный диск (***примечание***: *для ускорения процедуры восстановления рекомендуется предварительно скопировать bkf-файл с CD/DVD на HDD*).

В поле "Restore files to:" (куда восстанавливать) оставляем значение по умолчанию — "Original location" (исходная локация) и нажимаем кнопку "Start Restore", запуская процесс восстановления системы (см. рис. 9).

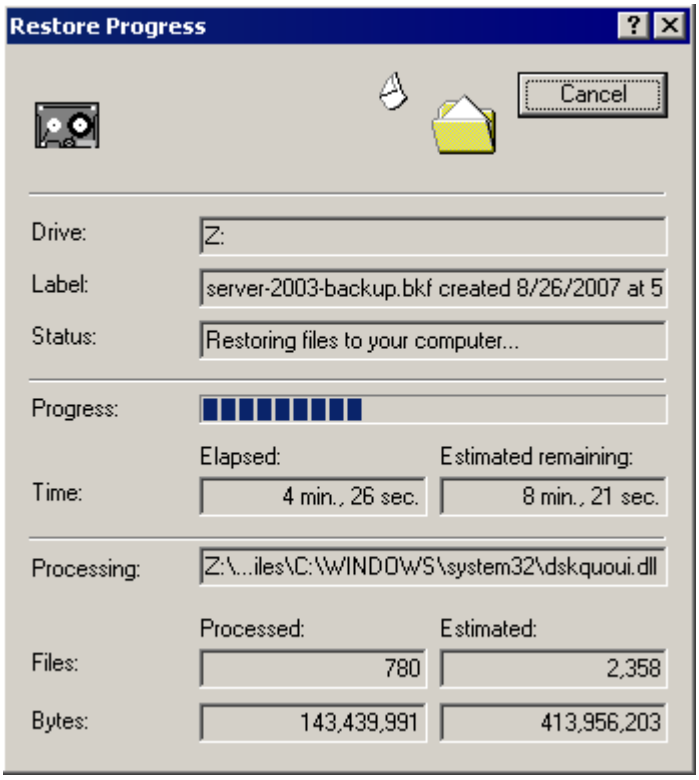

Рисунок 9 процесс восстановления системы в прогрессе…

После перезагрузки мы получаем нормально работающую систему.

тяжелые случае восстановления

Хорошо (то есть, на самом деле ничего хорошего), представим себе, что система не загружается. Ну не загружается и все тут, хоть грызи свой хвост, хоть бейся зубами об лед! Большинство администраторов, вылакав пол-литра корвалола, просто переустанавливают ее поверх старой или… даже страшно сказать — с нуля, забыв о том, что MS BackUp (который все ругают!) может ускорить эту работу в сотни раз!

Находим машину с любой стабильно работающей NT-подобной системой (W2K, XP, Server 2003, на счет Вислы мыщъх, правда, неуверен). Вставляем туда CD/DVD с архивом, запускам MS BackUp, переходим к вкладке "Restore and Manage Media" и (внимание!) в поле "Restore files to:" выбираем пункт "Alternative location" ("Альтернативное размещение"), указав любую папку, например, C:\TEMP\Server2003. Нажимаем "Start Restore" и… получаем копию системы только в другом месте.

Теперь подумаем: как перетащить все эти файлы на восстанавливаемый Server 2003. Путей на самом деле всего три. Снять жесткий диск с сервера и подключить его к рабочей машине вторым, после чего скопировать все файлы из папки Server2003 в каталоги Windows и (опционально) Program Files (***внимание****! файлы NTDETECT.COM и ntldr должны находится в строго определенных местах диска и потому их лучше не копировать, иначе система вообще перестанет загружаться*).

Естественно, если на сервере установлен хитрый SCSI или RAID, то подключить его к рабочей станции не удастся и в этом случае придется воспользоваться LiveCD, поддерживающим NTFS, например, KNOPPIX или Windows PE (о том, как самостоятельно создать диск с Windows PE рассказано в статье "восстановление данных на NTFS разделах", выложенной на http://nezumi.org.ru/recover.zip).

Если же RAID настолько хитрый, что его не видит даже KNOPPIX/Windows PE, то подключаем к рухнувшему серверу еще один жесткий диск, устанавливаем на его Server 2003 (со всеми необходимыми SCSI/RAID драйверами), перетягиваем туда по сети или через CD/DVD разархивированные файлы и осуществляем перезапись.

Как показывает практика, в подавляющем большинстве случаев, для восстановления системы достаточно переписать всего лишь реестр и классы, находящиеся в папках:

\temp\server-2003\Registry и \temp\server-2003\COM+ Class Registration Database. Скопируйте их в каталог \WINDOWS\system32\config поверх уже существующих файлов и перезагрузитесь.

Вот, собственно говоря, и все. При правильной организации вопроса, восстановление системы, которая даже не загружается, занимает не более 10-15 минут, расходуемых главным образом, на распаковку bkf-архива. Если же эту операцию выполнить заблаговременно, то на загрузку с LiveCD с последующим копированием реестра не уйдет и 5 минут!

ремонт bkf-архивов

Не то, чтобы очень часто, но все-таки случается, что MS Backup не может открыть bkf-файл, который сам же и создал. Причины могут быть самыми разными, но нас сейчас это не волнует! Единственная копия архива и та нерабочая! Как быть? Что делать? А на экран, тем временем, выдаются следующие злорадные сообщения:

- "The backup file is unusable. You must erase it, or choose another file" (архивный файл нестабилен, вы должны очистить его или выбрать другой файл);
- "The fixed media is full. You cannot back up all of the specified data to this disk device. The backup operation will stop" (несъемный носитель совсем заполнен. вы не можете сохранить все указанные файлы на этом устройстве, операция архивации будет остановлена);
- "The backup file contains unrecognized data and cannot be used" (архивный файл содержит нераспознанные данные и не может быть использован);
- "An inconsistency was encountered on the requested media" (архивный файл несовместим с данным носителем);

Поскольку, проблема возникла не вчера и даже не позавчера, то кричать "караул" не надо, а лучше воспользоваться одной из многочисленных утилит, предназначенных для "вытягивания" всей уцелевшей информации из bkf-файлов (а, как уже говорилось выше, в большинстве случаев нам достаточно вытянуть файлы, ответственные за хранение содержимого реестра, так что шансы на восстановления у нас есть и это очень хорошие шансы).

Ниже приводятся ссылки на производителей платный и бесплатных утилит. Какую из них выбрать — вопрос вкуса. Лично мыщъх предпочитает коммерческий пакет "Kernel BKF Recovery" от "Nucleus Data Recovery" (см. рис. 10) стоимостью в 129$. Другие пакеты не тестировал, так что не могу сказать о них ни хорошего, ни плохого.

- http://www.bkffilerecovery.com/
- http://www.recoverdatatools.com/ms-backup-recovery.html
- http://www.msbackuprecovery.net/

Рисунок 10 утилита для восстановления разрушенных bkf-файлов – одна из многих

>>> врезка полезный совет

Достаточно часто причиной сбоев системы становится повреждение учетной записи администратора, например, ветви реестра HKEY_CURRENT_USER, которую, кстати говоря, MS Backup _не_ архивирует. Иногда доходит до того, что администратора вообще не пускают в систему и приходится использовать различные утилиты (как правило, распространяемые за деньги) для восстановления пароля администратора или же переустанавливать систему, что отнимает уйму нервов и времени.

Но есть более простой путь — достаточно создать несколько учетных записей для пользователей, входящих в группу "администраторы" и если "поломалась" одна учетная запись, воспользоваться другой, благо, учетные записи администраторов на сервере обычно не содержат никаких уникальных персональных настроек, а если даже и содержат, то их, как правило, можно экспортировать/импортировать, но это уже слишком "высокие" материи, чтобы в них углубляться.

заключение

Рассмотрев вопросы, связанные с восстановлением системы, мы оставили за бортом проблему архивации пользовательских данных и документов, что так же можно сделать посредством MS BackUp, причем не только в ручном режиме, но и, например, по расписанию (см. рис. 11), однако, стратегия резервирования пользовательских данных далеко выходит за рамки темы нашего разговора и главным образом определяется политикой компании. Кто-то предпочитает держать все документы на сервере, используя системы контроля версий, обеспечивающих не только банальную архивацию, но и хранящих историю изменений, что крайне важно для совместной работы с документом.

Другие же хранят документы на рабочих станциях пользователей. Глупость конечно, вернее не глупость, а огромная головная боль для администратора, но именно эта глупость создает децентрализованную систему, способную функционировать даже при крахе сервера. В общем, вариантов много. А MS BackUp – всего лишь архиватор со встроенным планировщиком. Но… для поддержания сервера на плаву ничего другого и не надо!

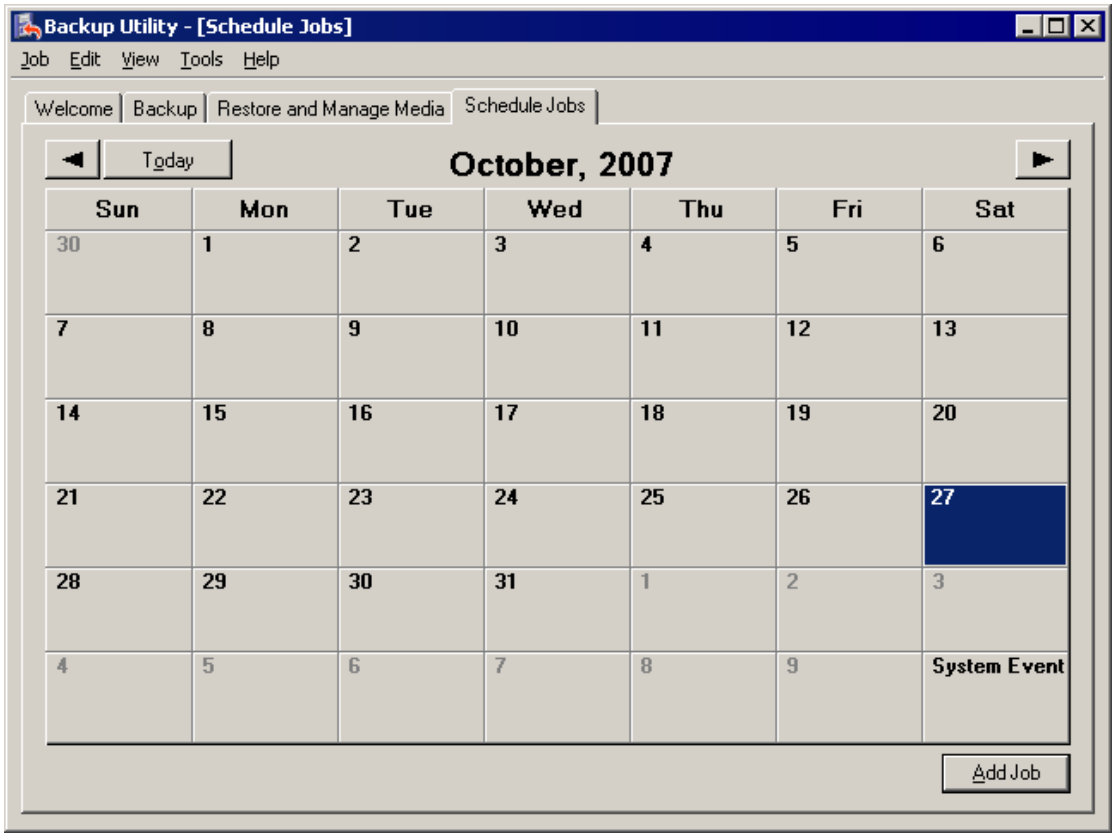

Рисунок 11 планировщик заданий, встроенный в MS Backup