

ЗЕМЕЛЬНЫЙ КАДАСТР

Version 1.0



Автоматизированная информационная система
ПРАВИЛА АРХИВИРОВАНИЯ
И ВОССТАНОВЛЕНИЯ ПОСЛЕ СБОЕВ

KZ.AS.00005-01 46 01

Содержание

Общие сведения.....	3
Рекомендации по обеспечению надежности хранения данных	4
Порядок выполнения резервного копирования.....	6
Порядок выполнения восстановления из резервной копии	8

Общие сведения

Для того, чтобы обеспечить сохранность данных в случае непредвиденных обстоятельств (поломка диска, сбой электропитания) необходимо регулярно производить *Резервное копирование (backup)* базы данных - считывание всех данных из базы данных и сохранение их в виде одного или нескольких файлов на диске. Обратный процесс - *Восстановление из резервной копии (restore)* - создание базы данных на основе информации, извлекаемой из файла резервной копии. Помимо сохранения данных от возможных опасностей, одновременное выполнение *backup/restore* предохраняет базу данных от "разбухания", служит для корректировки статистической информации, обеспечит меньшую фрагментацию базы данных, соответственно повышая ее быстродействие. Процесс *backup/restore* является обязательным участником всех профилактических и "лечебных" процедур обслуживания базы данных. Его регулярное выполнение уменьшает вероятность потери данных в будущем.

Частота процесса **backup** определяется администратором. Обычно он равен такому промежутку времени, за который данные, внесенные в БД не жалко потерять.

Процесс **restore** рекомендуется производить 1 раз в месяц.

Файлы резервных копий должны храниться на сменных носителях, CD, DVD – дисках, в крайнем случае – на другом компьютере (не сервере, где находится рабочая база данных).

ВНИМАНИЕ: Ни в коем случае не храните резервную копию на том же физическом диске, где находится рабочая БД. В случае сбоя диска, и рабочая БД и резервная копия могут быть повреждены, что приведет к полной утере данных!

Рекомендации по обеспечению надежности хранения данных

InterBase является транзакционной, клиент-серверной СУБД средних масштабов. В большинстве случаев она удовлетворяет потребности среднего предприятия, как по быстродействию, так и по надежности хранения данных.

Транзакционная схема взаимодействия пользователей с базой данных весьма надежно защищает ее от сбоев в результате некорректных действий пользовательских систем (программ + ОС). Т.к. Пользователь не имеет прямого доступа к файлу БД, он не может его испортить, удалив или выполнив некорректную операцию вследствие сбоев системы или электросети.

Но с другой стороны, на сервере, база данных – это всего лишь файл, а СУБД – всего лишь одна из программ (процессов) серверной ОС. И в этом случае надежность сервера как совокупности различных компонент (физических и программных), является слабым местом при обеспечении сохранности данных. В этом случае надежность сохранения информации в БД складывается из нескольких факторов:

1. Надежности энергообеспечения сервера
2. Надежности систем хранения данных
3. Надежности физических компонент сервера (оперативной памяти, процессора, магистралей передачи данных)
4. Надежности программной среды
5. Отсутствия постороннего неквалифицированного доступа к серверу

Рассмотрим каждый из этих факторов:

1. Надежность энергообеспечения, в самом простом случае, достигается подключением сервера через источник бесперебойного питания (ИБП) и установкой соответствующего ПО, которое в случае отсутствия напряжения и истощения батарей ИБП корректно завершит все приложения и выключит сервер.
2. В основном, современные накопители достаточно надежны, чтобы удовлетворить требования надежности при сравнительно небольших объемах хранимой информации (примерно до 500 Мб). Вкупе с регулярным резервным копированием этого достаточно. О большей надежности систем хранения можно думать, при значительных объемах информации и размерах предприятия. Для повышения надежности хранения данных используют различные вариации массивов данных с возможностью зеркального копирования данных, иногда, имеющих дополнительный резервный источник питания.
3. Надежность сервера, как набора проводов и микросхем – это, прежде всего, компьютеры известных фирм, либо компьютеры собранные из деталей, произведенных известными фирмами. Здесь можно порекомендовать компьютеры HP, Dell, Compaq. Либо компоненты «проверенных» производителей: Asus, SuperMicro, GigaByte, InWin, Seagate.
4. Здесь в первую очередь имеется ввиду наличие серверной операционной системы (Windows Server либо Linux-подобная ОС), для небольших предприятий – Windows XP, 2000. Крайне не рекомендуется Windows 98, ME, 95. Сюда же входит надежность программ, выполняемых на сервере – отсутствие вирусов, шпионов и пр., отсутствие установленных игр и пр. развлекательных программ.
5. Сервер баз данных, в идеальном случае, должен быть выделенным, в отдельном помещении и в сейфе под замком. Желательно, чтобы к нему не имели доступ посторонние, стояла система разграничения доступа по паролям, не запускались игры и пр. InterBase – СУБД совсем не требовательная и вполне допускает использование сервера БД как рабочего места пользователя. Но в этом случае

ответственность за порчу данных вследствие некорректных действий того же пользователя ложится на предприятие, принявшее подобное решение.

Несколько советов для малых предприятий, имеющих 2-3 компьютера и не имеющих постоянного обслуживающего персонала:

- Компьютер, на котором располагается БД, должен быть ОБЯЗАТЕЛЬНО снабжен ИБП.
- Рекомендуемая операционная система – Windows XP
- Рекомендуемая файловая система на диске, где хранится файл БД – NTFS.
- Обязательно наличие антивирусного и регулярно обновляемого ПО

Базы данных InterBase, как правило, поставляются с опцией кеширования изменений. Это способствует повышению быстродействия БД, но снижает ее надежность в случае сбоев работы сервера баз данных. Если ИБП отсутствует, рекомендуется переключить режим работы базы данных на прямую запись. Делается это с помощью командной строки:

```
<path1>\gfix -w sync -user SYSDBA -pa masterkey <path2>
```

(где, <path1> - каталог bin сервера InterBase; <path2> - полный путь к БД с указанием имени файла)

Режим кеширования включается строкой:

```
<path1>\gfix -w async -user SYSDBA -pa masterkey <path2>
```

Режим прямой записи снижает быстродействие, но значительно повышает отказоустойчивость базы данных при сбоях.

Порядок выполнения резервного копирования

	Действие	Комментарий
1	Убедитесь, что к базе данных, для которой будет выполняться резервное копирование, не подключены пользователи (не запущены клиентские программы).	
2	Резервное копирование необходимо выполнять на компьютере, где расположена БД, то есть на сервере InterBase.	
3	Нажмите Пуск->Выполнить, введите <code>cmd</code> , в открывшейся командной строке перейдите в каталог bin сервера InterBase. На экран будет выведено подобное сообщение: <code>C:\Program Files\Borland\InterBase\bin></code>	Выделенный путь должен соответствовать тому, куда установлен сервер на Вашем компьютере
4	Выполните команду вида (вводится в одну строку) <code>gbak -b -g <dbpath> <bkpath> -user sysdba -password <psw></code> где, <code><dbpath></code> - полный путь к БД, включая имя файла; <code><bkpath></code> - путь и имя файла резервной копии; <code><psw></code> - пароль пользователя SYSDBA на Вашем сервере.	
5	Дождитесь окончания выполнения процедуры резервного копирования. По окончании на экране командной строки должен появиться путь, откуда была запущена утилита GBAK: <code>C:\Program Files\Borland\InterBase\bin></code>	
6	Созданный в процессе резервного копирования файл <code><bkpath></code> запишите на внешний носитель и сдайте на хранение.	

Рекомендации

Backup - это изготовление резервной копии базы данных "на ходу". Выполнять можно при работающих пользователях, однако надо помнить, что сохранены в backup будут только те данные, которые существовали на момент старта backup. Делать backup (и restore) можно как через Services API (в IBConsole, IBExpert и других, или в Delphi в палитре компонент InterBase Admin), так и утилитами командной строки.

Например:

```
gbak -b localhost:c:\dir\db.gdb d:\db.gbk -user SYSDBA -pass masterkey
```

расширение файла backup значения не имеет. Не рекомендуется делать backup на тот же логический диск, где лежит база (если кончится место, и БД перестанет работать, и бэкап не сделается), а еще лучше делать backup на отдельный физический диск (с точки зрения производительности).

Быстрее всего backup можно получить, если выключить сборку мусора, которая работает по умолчанию:

```
gbak -b -g localhost:c:\dir\db.gdb d:\db.gbk -user SYSDBA -pass masterkey
```

(мусор никогда не попадает в backup. речь просто идет о том, что backup по умолчанию читая записи пытается определить, если у записи есть версии, то нужны они или нет, ключ -g отключает это поведение). Еще лучше всегда добавлять ключ -v, который приводит к подробному выводу действий backup - в этом случае если произойдет ошибка, будет видно, где именно она произошла. Вывод можно направить и в файл:

```
gbak -b -g localhost:c:\dir\db.gdb d:\db.gbk -user SYSDBA -pass masterkey -v -y bak-log.txt
```

Восстановление рекомендуется делать регулярно, и сохранять его в архив (лучший вариант - ежедневный backup с сохранением 7-ми последних копий).

Делать архив БД через простое копирование файла БД можно, только если к этой БД нет ни одного подключенного пользователя - файл БД это файл произвольного доступа, а копирование операционная система выполняет последовательно. В результате вы на выходе получите испорченную "копию" файла БД.

Порядок выполнения восстановления из резервной копии

	Действие	Комментарий
1	Убедитесь, что к базе данных, для которой будет выполняться восстановление из резервной копии, не подключены пользователи (не запущены клиентские программы).	
2	Восстановление из резервной копии необходимо выполнять на компьютере, где расположена БД, то есть на сервере InterBase.	
3	Нажмите Пуск->Выполнить, введите <code>cmd</code> , в открывшейся командной строке перейдите в каталог bin сервера InterBase. На экран будет выведено подобное сообщение: <code>C:\Program Files\Borland\InterBase\bin></code>	Выделенный путь должен соответствовать тому, куда установлен сервер на Вашем компьютере
4	Выполните команду вида (вводится в одну строку) <code>gbak -c -user sysdba -password <psw> <bkpath> <dbpath></code> где, <code><dbpath></code> - полный путь к БД, включая имя файла; <code><bkpath></code> - путь и имя файла резервной копии; <code><psw></code> - пароль пользователя SYSDBA на Вашем сервере.	
5	Дождитесь окончания выполнения процедуры резервного копирования. По окончании на экране командной строки должен появиться путь, откуда была запущена утилита GBAK: <code>C:\Program Files\Borland\InterBase\bin></code>	

Рекомендации

Не рекомендуется делать restore в файл оригинальной БД (ключ -r). Всегда делайте restore только с ключом -c.

Если backup будет каким-либо образом поврежден, восстановить из него базу данных вряд ли удастся.

Даже на нынешних рабочих станциях backup базы данных размером 2 гигабайта идет около 15 минут (с ключом -g). Если у вас этот процесс происходит как минимум в 2-3 раза дольше, значит сервер загружен другими задачами, у вас медленный винчестер, или проблемы какого-то другого рода.