Выпуск подготовлен для вас компанией Acronis

Acronis специальное издание

Backup для "Чайников"™

Вы узнаете:

- Ответы на частые вопросы о резервном копировании и восстановлении данных
- 10 советов по простому резервному копированию и восстановлению
- Как решить современные проблемы защиты информации, связанные с виртуализацией, облаками и ростом объема данных

Джоэл Берман (Joel Berman)

Друг Acronis

О компании Acronis

Своими решениями для резервного копирования, аварийного восстановления и безопасного доступа Acronis задает стандарты современных технологий по защите данных. На основе технологии создания образов и уникальной платформы AnyData Engine компания создает удобные, комплексные и безопасные продукты для резервного копирования файлов, приложений и операционных систем в любых средах — виртуальных, физических, облачных и мобильных.

Компания Acronis основана в 2002 году и сегодня помогает защитить данные более чем 5 млн. обычных пользователей и 300 тыс. корпоративных клиентов по всему миру. Компании принадлежит более ста уникальных патентов. Решения Acronis обладают широким спектром функций, включая миграцию, клонирование и репликацию, и признаны лучшими продуктами 2014 года такими авторитетными ресурсами, как Network Computing, TechTarget и IT Professional.

Дополнительную информацию см. на сайте **www.acronis.ru**. Читайте нас в Твиттере: **http://twitter.com/acronis_russia.**

Backup для "чайников"™

Acronis специальное издание

Автор: Джоэл Берман,
(Joel Berman)
Друг Acronis

WILEY

Backup *«для чайников»*® Acronis специальное издание

Издатель:
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-10186-4 (pbk);
ISBN: 978-1-119-10185-7 (ebk)

Произведено в Соединенных Штатах Америки

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie A. Johnson
Development Editor: Kathy Simpson
Acquisitions Editor: Katie Mohr
Editorial Manager: Rev Mengle

Business Development Representative: Sue Blessing
Custom Publishing Project Specialist: Michael Sullivan
Production Coordinator: Melissa Cossell

Содержание

Введение

Многие и сегодня уверены, что резервное копирование — это привычное всем создание простой копии данных. Возможно, так и было в 1960 году, когда инженеры изготовляли еще один набор перфокарт, и отправляли его на хранение в надежное место. Но за последние полвека технологии, а с ними и методы резервного копирования, шагнули далеко вперед. Теперь копирование нескольких файлов на другой диск и обратно необходимо только в самых элементарных случаях. Компании и простые пользователи все чаще доверяют свои данные специальным приложениям, которые способны справиться с восстановлением не только обычных файлов, но и больших сложных систем.

Об этой книге

В этой книге мы расскажем о современных способах защиты данных, опишем различные сценарии резервного копирования, разберем, какой из них выбрать лично вам и как правильно ему следовать. Конечно, это общее руководство, в котором нет ответов на по-настоящему специализированные вопросы, но книга «для чайников» их и не предполагает. Это гид, который станет для вас первоначальным проводником по установке и использованию защитных систем.

Сразу оговорюсь: «защита данных» — это общий термин, который означает резервное копирование и восстановление любой информации, включая файлы, программы и системное ПО. Не стоит путать его с шифрованием личной информации (например, данных кредитных карт или медицинских сведений). Кроме того, вам может встретиться термин «аварийное восстановление». Он означает восстановление всей системы после физического повреждения или масштабной хакерской атаки.

Под *защитой данных* мы подразумеваем хранение информации в правильных условиях. К таким условиям относятся максимально удобный поиск и возможность восстановить данные независимо от их локализации в архивах резервных копий. Термин *аварийное восстановление* означает быстрое восстановление сервера, рабочей станции или целого центра обработки данных после серьезного сбоя.

Смелые предположения

Когда я работал над этой книгой, то, конечно же, представлял себе будущего читателя. Вот, как я вас вижу:

- Вам знакомы информационные технологии (ИТ), но при этом вы не являетесь специалистом по защите данных.
- У вас есть некоторый опыт администрирования систем, но нет серьезной квалификации в этом деле.
- Скорей всего, вы хотите внедрить или оптимизировать резервное копирование в своей компании. Но для этого вам нужно разобраться с базовыми понятиями, получить советы по выбору правильных продуктов и рекомендации по их настройке.

Сноски, используемые в книге

Как и во всех книгах *«для чайников»*, сноски на полях указывают на определенный тип информации.

Текст, отмеченный значком «Совет», содержит полезные подсказки о принципах и методах резервного копирования.

Значок «Примечание» указывает на важные факты, о которых не следует забывать.

Текст, отмеченный значком «Техническое», читать не обязательно. Но лучше все же прочесть, поскольку это позволит вам лучше понимать механику резервного копирования.

Не пропускайте ничего под значком «Внимание!». Упустив важную информацию, вы рискуете потерять время, деньги или данные.

С чего начинать

Как и все книги *«для чайников»*, эту можно начинать с любой главы. Можно приступить к первой и идти по порядку или перелистывать главы и разделы — как вам будет удобнее.

Глава 1

Основы защиты данных

В этой главе

- Почему данные нуждаются в защите
- Какие данные следует защищать
- Что входит в систему резервного копирования

Важные корпоративные данные защищают от потери очень давно. Достаточно вспомнить машинописные копии документов, под которые еще несколько десятилетий назад отводились целые архивы. С тех пор многое изменилось, и не в последнюю очередь – методы защиты и восстановления информации. В этой главе вы узнаете о том, какие данные следует в первую очередь защищать и какие технологии для этого – самые подходящие.

О данных

Что такое данные? Вопрос может показаться простым, но ответить на него не всегда легко. Это могут быть и обычные текстовые файлы, и сложная информация самых разных видов. В этой книге под словом «данные» мы подразумеваем совокупность программ, файлов и метаданных, – так, как это делается в современных компьютерных системах.

Данные могут принимать любую форму, и нередко бывает сложно определить, что именно в них следует защищать. Как правило, в защите нуждается ценная информация. Пещерные люди старались уберечь свою добычу от волков и саблезубых тигров, а современный человек следит за тем, где оставляет дорогие наручные часы и паркует автомобиль. Мы бережем свои вещи, потому что они представляют для нас ценность. Если вещь потеряна или украдена, то, не найдя ее, мы в лучшем случае можем вернуть ее стоимость благодаря страховке. К счастью, с данными дело обстоит не так. Если позаботиться о них должным образом, то можно легко восстановить необходимую информацию в изначальном объеме.

Защита данных

В работу ИТ-специалиста входит защита данных от потери и повреждений: например, при краже, случайном удалении или намеренном редактировании. Защитить данные проще, чем может показаться. Если выбрать правильную стратегию и придерживаться ее, то информация будет защищена на любом уровне и практически от любых случайностей.

Для начала рассмотрим, какие элементы следует защищать.

- **Данные начальной загрузки.** Это данные, которые используются при запуске машины; программа, которая запускается в первую очередь при включении или перезагрузке системы. Если что-то случится с ней, система не сможет работать.
- **Метаданные файловой структуры.** Эти данные описывают расположение всех файлов и папок в системе. В том числе – файлов начальной загрузки, файлов операционной системы и драйверов. В метаданных записано, какие блоки на диске используются, а какие свободны. Каждое имя файла и папки сопоставлено в них с конкретным местом на диске. Кроме того, данные этого типа содержат списки доступа к документам и предотвращают неавторизированные чтение и запись. Метаданные важны для полного восстановления системы.

  

  В некоторых системах история изменений записывается в специальные журналы аудита. Эти журналы используются для восстановления системы после сбоев питания и других внезапных остановок.
- **Двоичные файлы драйверов.** Эти файлы управляют устройствами чтения с дисков, лент или из сети. Драйверы, как правило, являются частью операционной системы и должны быть с ней совместимы. Часто они поставляются вместе с отдельными комплектующими и не входят в ОС изначально.
- **Операционная система.** Код ОС, как правило, поставляется на физическом диске. Производители часто выкладывают обновления ОС в сеть, поэтому исходный диск рано или поздно устаревает.

  

  Важно создавать резервные копии ОС после каждой установки обновлений, чтобы всегда иметь под рукой самую последнюю версию. Иначе, после реанимации системы, вам придется запускать все обновления заново, а это долгий и трудоемкий процесс.

- **Файлы конфигурации.** Существует множество файлов конфигурации: это и простые файлы, содержащие имя системы или часовой пояс, и огромные файлы с тысячами элементов – такие, как реестр Windows. К этому типу относятся также файлы паролей. Некоторые программы так сильно защищены, что при утере пароля восстановление данных становится невозможным. Кроме того, многие приложения используют сложные файлы конфигурации, в которых хранится самая разнообразная информация о системе.
- **Программные приложения.** Большинство компаний приобретает программы у сторонних производителей. Самый простой пример – Microsoft Office или программы бухгалтерского учета. Но некоторые фирмы разрабатывают свои собственные приложения. Самое неприятное, что может с ними случиться, это потеря исходного кода. Если компания лишится файлов, кодирующих уникальную программу, то все сохраненные с ее помощью данные окажутся бесполезными. Вывод: приложения тоже необходимо защищать.
- **Файлы данных.** Файлы данных — обычные файлы, которые используются многими программами. Это могут быть электронные таблицы, изображения, текстовые или PDF-документы, а также файлы журналов, с которыми работают специальные приложения. Файлы данных бывают объемными или небольшими, неизменными или постоянно редактируемыми. На любом корпоративном сервере их могут быть сотни тысяч и даже миллионы.
- **Базы данных.** Базы данных можно рассматривать как самостоятельные приложения с файлами, однако они постоянно обновляются и потому нуждаются в особых способах защиты, обеспечивающих синхронизацию.

Просто, комплексно, безопасно

Три главных принципа резервного копирования — это простота, комплексность и безопасность. Рассмотрим их поподробнее.

Простота в работе

Простота является самым важным качеством резервного копирования. Чем проще схема, тем меньше шанс допустить в ней ошибку. Трудно представить, сколько раз данные восстанавливали из устаревших копий или перезаписывали неправильную информацию поверх правильной, – и все потому, что кто-то пытался в спешке следовать сложным, плохо прописанным процедурам. Чтобы избежать этого,

стоит помнить о четко прописанных алгоритмах и контрольных списках восстановления. Компаниям, которые много лет занимаются резервным копированием своих данных, необходимо следить, чтобы для этого не использовались несовместимые продукты и носители.

Простой и удобный интерфейс – серьезное преимущество. Если можно приступить к работе без долгих настроек или восстановить систему одним щелчком мыши, это большой плюс, который может перевесить даже наличие четких контрольных списков.

Комплексность

Комплексность резервного копирования подразумевает:

- защиту различных данных в любом месте и в любой среде
- избавление от лишних действий

Например, при восстановлении, программа должна воспроизводить форматы и разделы дисков, а не предлагать вам сделать это вручную (поскольку это непростая задача, которая требует безупречного исполнения).

Хорошая программа должна обладать максимальным набором инструментов. Ваше ПО для резервного копирования может создать загрузочный CD- или DVD-диск, который понадобится для восстановления при неработающей системе. Если программа не позволяет создать загрузочный диск, придется переустанавливать систему прежде, чем запускать восстановление, а это, конечно же, отнимет лишнее время.

Наконец, – но не в последнюю очередь – ПО для резервного копирования должно давать четкие инструкции. Вы будете следовать им, как командир экипажа при экстренной посадке самолета.

Любые данные, среды, места и устройства

Хотя виртуализация существует больше 30 лет, ее бурное развитие пришлось на последнее десятилетие. В 1999 году компания VMware выпустила свой первый программный гипервизор. С тех пор появилось множество других гипервизоров, а производители стали переносить программные функции на аппаратную часть оборудования, чтобы повысить производительность системы. Увеличение плотности оперативной памяти и многоядерные процессоры позволяют использовать все большее число рабочих нагрузок: сегодня они могут легко переноситься из физической среды в виртуальную и обратно с помощью различных гипервизоров и облачных технологий.

В условиях быстрого развития, ПО для защиты данных и аварийного восстановления (DP/DR) должно работать и в физической, и в виртуальной среде и поддерживать популярные гипервизоры. Только такое ПО сохранит архивы резервных копий в рабочем состоянии независимо от фактического расположения нагрузки. Непременное условие – способность переносить операционные системы, приложения и данные между физическими, виртуальными и облачными средами с использованием любого гипервизора. Выбирайте решение для резервного копирования, которое будет работать со всеми данными, любыми средами и устройствами.

Уверенность в безопасности

Безопасность резервного копирования включает в себя два аспекта:

- **Надежность.** Мало сохранить резервную копию: нужно, чтобы она была доступна для восстановления. ПО для копирования может использовать самые разные методы для переноса данных, но если они будут не читаемы, восстановить систему не удастся. Единственный отсутствующий фрагмент может сделать всю вашу работу по сохранению бесполезной.
- **Защищенность.** Даже после того, как данные сохранены, их нужно дополнительно защищать – от вторжения и кражи. Если система резервного копирования не рассчитана на это, злоумышленник может легко взломать ее, украсть данные или повредить основную систему.

Как известно, профилактика лучше лечения. Старайтесь не усложнять процесс резервного копирования и тщательно его документируйте. Начните с первых шагов и в точности следуйте алгоритму (см. главу 2). Если вы сохраните данные неправильно, то потом не сможете их восстановить.

Глава 2

Сохранение данных при резервном копировании

В этой главе

- Резервное копирование файлов и образов
- Настройка плана резервного копирования
- Резервное копирование с агентами и без них
- Выбор решения для резервного копирования

Для большинства из нас резервное копирование — это сохранение нескольких самых важных файлов на отдельном диске или флэш-носителе. Однако большие системы и серверы содержат множество файлов, которые постоянно изменяются. Чтобы при случае восстановить потерянные или поврежденные данные, нужно регулярно сохранять их копии. Это необходимо даже тогда, когда файлы открыты и редактируются.

В этой главе мы подробно рассмотрим основные типы резервного копирования, обсудим их применение и особые сценарии использования.

Типы резервного копирования

Существует два основных способа сохранения данных — резервное копирование образов и резервное копирование файлов. Рассмотрим их по порядку.

Оба метода позволяют выполнять поиск определенных файлов и данных. Однако резервное копирование образов является расширенной версией, поскольку предполагает работу с метаданными системы и дает дополнительные возможности при восстановлении.

Большинство устройств для хранения данных, кроме ленточных накопителей, воспринимается низкоуровневым ПО как диски. К примеру, CD/DVD-устройства имеют особые условия записи, но все равно распознаются как диски, то есть последовательность блоков. Оборудование передает эту последовательность операционной системе, причем каждый блок может считываться и записываться отдельно. Внутри некоторых блоков находятся *метаданные*, которые содержат папки, списки используемых, свободных и поврежденных блоков, данные начальной загрузки, информацию о разделах диска, а также сведения о сопоставлении.

Даже если диск только что отформатирован, некоторое место на нем все равно занимают метаданные. Именно поэтому свободное пространство на дисках оказывается меньше емкости, заявленной производителем.

Резервное копирование файлов

Резервное копирование файлов — это самый старый и до сих пор популярный способ застраховать информацию от потерь. Все файлы и папки копируются на резервный носитель, что очень похоже на обычную перезапись личных файлов на внешний диск или в другую папку на компьютере.

Поскольку в файловой системе хранится информация о времени создания и изменения каждого файла, при копировании можно обрабатывать только те документы и папки, которые были изменены со времени записи предыдущей копии. Для программы резервного копирования это нетрудная задача, ведь ОС предоставляет для этого все необходимые инструменты. Однако нужно учитывать, что перезапись файлов значительно нагружает систему, так как для каждого файла нужно произвести целый ряд действий:

1. **Найти блоки, в которых расположены папки.**
2. **Прочитать папки.**
3. **Найти имена файлов.**
4. **Определить расположение файлов.**
5. **Прочитать и скопировать соответствующие блоки.**

Все это может занять много времени. Если одновременно выполняются другие процессы, производительность всей системы может заметно упасть.

Резервное копирование образов

Резервное копирование образов позволяет избежать большей части нагрузки на систему, неизбежной при поиске файлов. Полная копия диска создается простым копированием блоков по очереди. Причем программа распознает и копирует только те блоки, которые были изменены со времени создания последней копии. Так, если в файле размером 2 ГБ сделано небольшое изменение, то при резервном копировании файлов будут перезаписаны все 2 ГБ, а при резервном копировании образа — только измененный блок. Благодаря такому алгоритму резервная копия создается очень быстро.

Самые быстрые программы для резервного копирования сохраняют данные только из используемых блоков. Они не копируют поврежденные, временные, неизменные и неиспользуемые блоки, если это напрямую не задано пользователем.

Технология резервного копирования образа обычно позволяет отображать копию, как дополнительный диск. Администратор может просмотреть его содержимое и при необходимости восстановить отдельные файлы.

Резервные копии образов и файлов могут быть полными, дифференциальными или инкрементными. Все три типа позволяют исключить из копирования отдельные виды данных, если они вам по каким-то причинам не нужны (например, временные файлы). О типах резервных копий мы поговорим в следующем разделе.

Изначально образы назывались *моментальными снимками*, однако сегодня у этого термина есть два значения, и, чтобы избежать путаницы, лучше говорить *резервная копия образа*, а не *резервная копия снимка*. О снимках можно прочесть в разделе «Создание моментального снимка».

Резервное копирование по плану

В плане резервного копирования определяются данные, которые необходимо сохранить, и область их расположения (тот или иной диск, виртуальная машина и т. д.). В этом разделе мы рассмотрим несколько вопросов, которые нужно решить, чтобы составить оптимальный план резервного копирования.

Выбор между полным, дифференциальным или инкрементным резервным копированием

Существует три типа резервных копий:

- **Полные.** Полная копия — это резервная копия системы с сохранением всех данных. Достоинство такой копии в ее автономности. Среди недостатков — большой размер, долгий процесс создания и нередко – почти полная идентичность с предыдущей полной копией.
- **Дифференциальные.** В дифференциальной резервной копии сохраняются различия между текущим состоянием системы и ее последней полной копией. Для восстановления из дифференциальной копии нужно, чтобы последняя по времени полная копия также была рабочей.

  Преимущество дифференциальной копии в сравнительной быстроте создания. Однако такая копия может иметь довольно большой размер. Кроме того, для восстановления из нее понадобится обработать как минимум два файла резервных копий.
- **Инкрементные.** В инкрементной резервной копии сохраняются различия между текущим состоянием системы и любой последней по времени резервной копией. Последняя копия может быть полной, дифференциальной или тоже инкрементной – для инкрементного копирования это не важно.

  Достоинства инкрементной копии – компактный размер и высокая скорость создания. Неудобство же в том, что для восстановления из такой копии необходима обработка последней полной копии и каждой последующей инкрементной – вплоть до *директивной точки восстановления* (про нее см. следующий раздел). В результате восстановление системы из резервных копий этого типа может занять очень много времени.

Большинство современных программ для резервного копирования позволяет объединять инкрементные копии в автономном режиме. Это значительно повышает надежность копирования и ускоряет процесс восстановления. Резервное копирование с автоматической консолидацией при создании копий называется *обратно-инкрементным*. Еще один новый тип резервного копирования — *всегда инкрементный* (хотя стоит отметить, что разные поставщики трактуют этот термин по-разному).

В большинстве случаев размер ежедневной инкрементной копии, составляет 3–5 % от размера полной. Однако эти цифры могут сильно отличаться в зависимости от вида данных, с которыми работает ваша компания. К тому же, после значительных изменений (например, после обновления ПО), размер инкрементной копии может стать больше. При подготовке серьезного обновления системы, приложений или данных лучше всего выполнить полное резервное копирование: одно перед внесением изменений и еще одно — сразу после. Если вы собираетесь экспериментировать с системой, создавайте резервные копии чаще.

RPO и окно резервного копирования

Временной промежуток, через который необходимо создавать резервную копию данных, определяется *директивной точкой восстановления* (RPO, Recovery Point Objective). Для разных систем и рабочих нагрузок она может быть разной: и пять минут, и час, и целые сутки. Если значение RPO составляет 30 минут, точка восстановления должна создаваться каждые полчаса. Так как создание резервной копии требует больших вычислительных ресурсов, работа остальных приложений должна на какое-то время приостановиться. На несколько часов, или на несколько секунд – зависит от плана и метода резервного копирования, мощности системы и даже от характера вашего бизнеса. Время, на которое работу системы можно приостановить для создания копии, называется *окном резервного копирования.*

Чем меньше значение RPO, тем короче должно быть окно копирования. Оно и понятно: частые точки восстановления провоцируют остановки или замедление работы, и это замедление должно быть, по возможности, кратким. Хорошо, если резервная копия создается раз в сутки после окончания рабочего дня, однако многие процессы требуют копирования при работающей системе с изменяющимися данными. К счастью, есть технологии, которые позволяют устранить окно резервного копирования и исключить необходимость приостановки системы. О них мы поговорим ниже, после того, как выясним, как правильно рассчитать RPO.

Есть множество методов, позволяющих сократить окно резервного копирования и создавать точки восстановления чаще. Однако все они требуют значительных ресурсов. Чтобы выполнять рабочие операции одновременно с копированием, система должна быть достаточно мощной. Современное ПО позволяет ограничить потребление ресурсов системы при записи копии, однако сама копия из-за этого создается медленнее.

Расчет RPO: оценка расходов, преимуществ и рисков

Чтобы определить оптимальную для вашей компании RPO, придется тщательно взвесить несколько факторов. Кроме

объективной необходимости сохранять копию данных, стоит учесть:

- стоимость простоя оборудования
- стоимость невыполненной работы
- стоимость самого применения RPO (расходы, связанные с созданием резервных копий)

Стоит помнить и про такой нематериальный, но вполне ощутимый риск, как потеря репутации. Если ваша компания позиционирует себя, как поставщик недорогих услуг, то не исключено, что частое резервное копирование для нее – ненужная роскошь. Если же реклама компании обещает полное отсутствие сбоев и железную сохранность данных, то даже несколько минут простоя, потеря единственного документа или транзакции могут повредить ее деловому имиджу.

Если для вашей компании важна возможность восстановления системы на любой момент времени, вам придется хранить огромное количество резервных копий. В этом случае удобно использовать скользящее значение RPO. Например, для критически важных рабочих нагрузок можно установить следующие значения: каждые пять минут на ближайшие 24 часа, каждый час – на ближайшие несколько дней, ежедневно – на следующий месяц и ежемесячно – на все остальное время. Для менее важных рабочих нагрузок или нагрузок, которые редко меняются, можно задать ежедневное создание RPO в первую неделю и ежемесячное — после. Помните, что с течением времени самые старые точки восстановления удаляются.

Если вы в принципе не хотите допустить потери каких-либо данных, имейте в виду, что решение этой задачи может обойтись очень дорого. Само по себе резервное копирование не гарантирует полного отсутствия сбоев и нулевого времени простоя. Для этого потребуется больше оборудования, вспомогательные сайты и специально разработанные системы.

Самый простой способ сократить окно резервного копирования, не жертвуя оптимальным значением RPO — использовать метод моментальных снимков (см. следующий раздел).

Создание моментального снимка

Вполне очевидный способ ускорить резервное копирование — свести к минимуму объем копируемых данных. Для этого программа совсем ненадолго приостанавливает работу системы и создает *«моментальный снимок»* – *копию* метаданных с описанием расположения всех файлов на машине или сервере.

После создания снимка копирование самих данных идет в фоновом режиме: программа обращается к снимку, как к указателю, чтобы найти и перезаписать тот или иной файл или блок.

Моментальные снимки сильно сокращают окно резервного копирования и потому особенно полезны при частых обновлениях системы. Этот метод подходит и для управления сетью хранения данных (SAN): ресурсы SAN активно используются для общей работы, и, если они недоступны дольше нескольких секунд, производительность системы резко падает.

Вместе с тем, у копирования методом моментального снимка есть один недостаток. После создания снимка исходные данные могут меняться (например, могут быть созданы новые файлы), после чего исходные метаданные будут обновлены, а их копия в моментальном снимке — нет. В результате система резервного копирования «не увидит» новые данные и не сохранит их. На этом фоне полное или хотя бы инкрементное резервное копирование надежней, хотя оно и займет намного больше времени и потребует прерывания всех операций.

В целом надо отметить, что моментальные снимки не могут применяться постоянно: это метод для особых случаев. К тому же их удаление требует значительных ресурсов.

Моментальный снимок не является полной копией данных. Если исходный диск повредится, снимок тоже будет поврежден. Поэтому снимки подходят только для временного использования и не могут служить заменой резервным копиям.

Некоторые приложения помогают дополнительно сократить окно резервного копирования при создании моментального снимка. Так, решения VMware отслеживают измененные блоки по технологии CBT, благодаря чему копирующая программа тратит меньше времени на сохранение данных. Другой пример – служба теневого копирования томов Microsoft (VSS). Рабочие приложения и программа резервного копирования должны поддерживать эти технологии, иначе создание полной резервной копии будет невозможно.

Резервное копирование с агентами и без них

Программы для резервного копирования могут обращаться к данным системы двумя способами.

- **С помощью агента.** В этом случае на каждую физическую и виртуальную машину (ВМ) устанавливается небольшая программа-агент.

- **Без агента.** В облачных и виртуальных средах количество ВМ может быть довольно большим, поэтому здесь удобнее использовать *резервное копирование без агентов*.

Во втором варианте агенты также используются, но в очень небольшом количестве, а значит, процессом копирования проще управлять. Как правило, агент устанавливается на каждый виртуальный хост, который тоже располагается на виртуальной машине. Агент обменивается данными с хостом и копирует все расположенные на нем ВМ. В большинстве систем несколько хостов, и ВМ могут перемещаться между ними, поэтому системы резервного копирования должны постоянно отслеживать их положение.

Резервное копирование без агентов очень удобно. Однако есть случаи, когда хост или гипервизор не может скопировать некоторые объекты, связанные с ВМ. Тогда приходится устанавливать агент непосредственно на виртуальную машину.

Убедитесь, что на виртуальных машинах установлено необходимое число агентов. Регулярно обновляйте их и, если необходимо, поддерживайте базу лицензий.

Выбор решений для резервного копирования

Изначально резервное копирование образов выполнялось одним приложением, а резервное копирование файлов — другим. Сегодня хорошее ПО для копирования легко справляется с обеими задачами. Современные программы создают резервные копии образов полного, дифференциального и инкрементного типа, а также используют моментальные снимки, чтобы сократить окно резервного копирования (см. ранее в этой главе). Такие программы могут сохранять данные на уровне блоков, а затем восстанавливать файлы из созданного образа.

В первую очередь, старайтесь создавать резервные копии образов, а резервные копии файлов — только если для этого есть объективные причины. Например, некоторые сетевые диски и системы хранения SAN и NAS не позволяют выполнять копирование образов из-за того, что у агентов копирования нет программного доступа к метаданным.

Хорошее приложение для резервного копирования может восстановить весь образ на новую систему. Более того, оно может скорректировать образ, исходя из размеров нового диска, и внедрить в систему нужные драйверы. При восстановлении на другое оборудование приложение меняет параметры начальной загрузки и настраивает систему на новые условия: другой тип

процессора, контроллеры устройств, конфигурацию хранилища и оперативную память.

Самые быстрые программы резервного копирования сохраняют данные только из используемых блоков, пропуская неиспользуемые и поврежденные.

Восстановление на «голое железо»

«Голое железо» — это система, на которой не установлено никакого программного обеспечения. На такую систему можно восстановить только резервную копию образа, поскольку резервная копия файлов не содержит всех метаданных и параметров начальной загрузки. Копию образа можно восстановить на «голое железо», даже если она была создана на машине с другими характеристиками. Кроме того, современные программы резервного копирования позволяют преобразовать физический образ в виртуальный и наоборот. Актуальная опция – экспорт виртуального образа в любую популярную систему виртуализации.

Поинтересуйтесь у своего поставщика, использует ли он универсальный формат резервных копий, который можно восстанавливать и на физические, и на виртуальные машины.

Однопроходное резервное копирование

Однопроходное резервное копирование — тип копирования, при котором для создания резервной копии и восстановления требуется только одно считывание данных. Само собой, такое копирование быстрее многопроходного, что позволяет создавать точки восстановления чаще.

Если продукт включает резервное копирование и образов, и приложений, то данные, необходимые для полного восстановления системы, можно сохранить за один проход. И наоборот: три отдельных однопроходных продукта для копирования образов, файлов и приложений, потребуют трех проходов, чтобы сохранить все данные. При этом информация будет храниться в разных архивах и управлять ею придется по-отдельности. Такой вариант создает дополнительные сложности и увеличивает риск сбоя при восстановлении.

Требования при сохранении данных

Прежде чем настраивать сохранение данных, нужно определить:

- ✓ RPO для каждой подсистемы и приложения;
- ✓ окно резервного копирования или допустимую продолжительность простоя;
- ✓ тип резервного копирования (копирование образов или файлов, или то и другое вместе);
- ✓ обрабатываемые приложения;
- ✓ максимальное число процессов резервного копирования, которыми можно успешно управлять.

Бывает, что для резервного копирования разных типов данных (образов, физических и виртуальных машин, облачных приложений, баз данных, электронной почты и документов) требуются разные программы и процессы управления. В результате файлы резервных копий оказываются несовместимы, что подвергает риску всю вашу информацию. Быстрое развитие вычислительных систем, внедрение новых архитектур и типов оборудования позволяет решить эту проблему. Однако компании зачастую не спешат переносить данные на новые системы из-за сложности и дороговизны этого процесса. Учитывая это, стоит выбирать продукт, который работает с любыми данными и в разных вычислительных средах: может сохранять системы, программы и данные с любых гипервизоров, физических или виртуальных машин.

Глава 3

Безопасное хранение резервных копий

В этой главе

- Настройка политики хранения данных
- Выбор ПО, оборудования и сайтов
- Сжатие и дедупликация данных
- Оценка стоимости хранения

Проверенный временем принцип резервного копирования — *правило 3-2-1*, которое гласит: храните три копии данных на двух разных типах носителей, при этом одну копию храните в удаленном хранилище.

Раньше в качестве носителей использовались ленты и диски, но в современных компаниях их постепенно вытесняют облачные хранилища. Возможность хранить большие объемы данных и низкая стоимость — очевидные преимущества облачных технологий. Облако — это одновременно и другой тип носителя, и внешнее хранилище. Оно особенно подходит для хранения небольших объемов данных, поскольку делает стоимость локального архива резервных копий минимальной. Это не значит, что ленточные носители ушли в прошлое, однако облако все чаще используется в качестве альтернативы. В начале работы, когда данных немного, серьезных вложений для резервного копирования в облако не требуется.

Создание политики резервного копирования

Возможно, в вашей компании уже есть та или иная политика резервного копирования. Но если вы собираетесь внедрять новые технологии, вам, скорей всего, потребуется усовершенствовать привычные методы работы. В этом разделе вы найдете советы по настройке эффективных политик и планов резервного копирования.

План резервного копирования

План резервного копирования содержит информацию о том, какие данные следует обрабатывать и как часто это нужно делать. В зависимости от ваших потребностей план может быть очень простым или, наоборот, довольно сложным.

- Самый простой план резервного копирования подразумевает создание полной резервной копии образа ежедневно в полночь.
- Пример более сложного плана: полная резервная копия создается раз в неделю, дифференциальная копия — каждую ночь, а инкрементные копии — каждые четыре часа. При этом резервное копирование на машинах А и Б может начинаться в 10 часов вечера, на машинах В и Г — в полночь, а на машинах Д и Е — в два часа ночи: все с произвольной задержкой не более двух часов. *Сведения о полных, дифференциальных и инкрементных резервных копиях можно найти в главе 2.*
- Еще более сложный план: резервные копии образа системы создаются еженедельно, системы Windows Exchange — непрерывно, системы Microsoft SharePoint — каждую ночь. При этом пользовательские файлы копируются через день по произвольному расписанию, данные конфигурации системы и виртуальных хостов — еженедельно, а данные Active Directory — каждые восемь часов.

Хороший план должен содержать достаточное количество таких произвольных параметров, как ограничение загрузки сети. В нем также указывается, что системы, отключенные для экономии электроэнергии, должны включаться при активности в локальной сети (LAN). Кроме того, в плане отмечается, какие действия следует выполнять при обнаружении ошибок. Например, аварийное резервное копирование может запускаться, если в журнале Windows появляются ошибки диска.

Важно, чтобы план резервного копирования обладал достаточной гибкостью. Однако, при выборе программ для копирования, лучше выбирать те, которые уже включают стандартные настраиваемые планы. Так, если вам нужны полные резервные копии образов, используйте программу, которая позволяет создавать из них виртуальные машины (ВМ). *Подробнее см. раздел о виртуализации далее в этой главе.*

Политика хранения

Политика хранения – это ключевая часть любого плана резервного копирования. Скорей всего, вы не можете вечно хранить все копии, и рано или поздно вам придется удалять точки восстановления, чтобы освободить место для новых. Политика хранения определяет, что и когда удалять.

Самая примитивная политика хранения заключается в удалении старых резервных копий, когда места становится недостаточно. Сложность этой процедуры состоит в правильном выборе.

В следующих разделах мы поговорим о двух распространенных типах политик хранения.

«Дед-отец-сын» (GFS)

Представим простую схему: каждый день вы создаете одну резервную копию; к концу недели у вас есть семь копий, но при этом места в хранилище стало меньше. Вы берете одну из ежедневных копий, переименовываете ее в еженедельную, и продолжаете создавать ежедневные копии. К концу второй недели вы берете последнюю ежедневную копию и снова переименовываете ее в еженедельную, продолжая создавать ежедневные копии. Таким образом, в любой момент времени к вашим услугам ежедневные или еженедельные резервные копии. Однако свободное место в хранилище все равно сокращается, поэтому каждые четыре недели вы переименовываете последнюю еженедельную копию в ежемесячную и продолжаете следовать плану.

Этот тип политики называется *«дед-отец-сын» (GFS, Grandfather-Father-Son).* Ежедневные резервные копии — это «сын», еженедельные — «отец», а ежемесячные — «дед».

При достаточно долгом применении этой политики место в хранилище рано или поздно закончится, и придется что-то удалить. Но что именно? Если вы не готовы ответить на этот вопрос, возможно, вам подойдет следующая политика.

«Ханойская башня» (ToH)

«Ханойская башня» (ToH, Tower of Hanoi) – так называется детская игра, в которой нужно переместить пирамиду из дисков с одного стержня на другой. При этом за раз можно перемещать только один диск, и класть больший диск на меньший не разрешается. Последовательность ходов для решения этой головоломки представляет собой двоичный алгоритм.

Политика *«Ханойской башни»* позволяет повторно использовать пространство хранилища и размещать резервные копии на разных носителях. Ведь если все ежедневные, еженедельные и ежемесячные резервные копии лежат на одном диске, то, при общем сбое системы и этого диска, вы потеряете все данные. Чтобы не складывать яйца в одну корзину, носители лучше чередовать.

На практике «Ханойская башня» используется реже, чем следовало бы; в первую очередь, из-за трудностей управления. Подробности работы с этой политикой настолько сложны, что выходят за рамки данной книги. Тем не менее, некоторые программы для резервного

копирования предлагают использовать эту политику в автоматическом режиме. Я бы посоветовал выбирать именно такие.

Некоторые программы просто удаляют самые старые точки восстановления. Несмотря на видимую простоту, этот способ освобождения места не является оптимальным. Необходимо хранить хотя бы несколько старых резервных копий. Они могут пригодиться, если обнаружится проблема, существовавшая многие месяцы или даже годы.

Выбор ПО для резервного копирования

При выборе ПО для резервного копирования, обратите внимание на следующие функциональные преимущества:

- **Количество вариантов восстановления.** Например, при резервном копировании базы данных SQL, у вас должна быть возможность подключить файл резервной копии, как базу данных, чтобы сразу же начать ее использовать. Если вы подозреваете, что резервная копия образа диска содержит вирусный код, программа должна подключить образ, как диск, и позволить вам выполнить антивирусное сканирование.
- **Отсутствие нужды в переустановке.** Некоторые решения для резервного копирования не поддерживают копирование и восстановление хостов виртуализации VMware, Windows или Linux. При этом поставщики таких решений могут утверждать, что установить гипервизоры с нуля очень просто. Это так, но при условии, что у вас есть нужные программы и выработанные навыки, хорошие инструкции и все необходимые параметры конфигурации. Гораздо легче выполнить резервное копирование образа виртуального хоста без переустановок, чтобы потом просто загрузить его и начать работать.
- **Совместимость с оборудованием ваших систем.** Ранние серверы были очень требовательны к конфигурации ОС и при неверных параметрах просто-напросто не запускались. Сегодня появилось больше возможностей для стандартизации, и современные операционные системы могут выполнять автоматическую подстройку параметров для разного оборудования.

  

  Если вы приобретаете оборудование другого производителя или иного поколения, убедитесь, что ваше ПО для восстановления с ним совместимо.
- **Совместимость с вашими системами виртуализации.** Если вы выполняете резервное копирование образов или виртуальных

дисков, у вас должна быть возможность восстановления как на виртуальные, так и на физические машины.

Для этого подойдет ПО, которое после резервного копирования может экспортировать файл ВМ и поместить его в программу управления виртуальными машинами вашего гипервизора. Если возникнет необходимость восстановить систему до более ранней точки, ВМ уже будет готова к запуску.

Выбор носителя резервных копий

Чтобы выбрать подходящий носитель, нужно понять, сколько места потребуется для хранения ваших резервных копий. Приведем несколько рекомендаций.

Необходимый объем хранилища зависит от числа резервных копий, срока их хранения, скорости, с которой данные меняются и растут в объеме. В некоторых отраслях на эти показатели есть специальные нормативы. Для начала выделите объем, в 3–5 раз превышающий текущий объем данных. В течение нескольких месяцев внимательно наблюдайте, а затем составьте план на будущее.

Если вам нужны более точные сведения, измерьте объем своих данных и подумайте о преимуществах сжатия и дедупликации. Следите за тем, сколько новых данных копируется ежедневно в течение нескольких недель. На основании этого вы определите нужное число резервных копий для хранения и необходимый срок их давности.

После того, как вы рассчитаете объем хранилища, можно выбрать подходящий носитель. Есть три варианта носителей: диски, ленты и облака. Каждый из них имеет свои преимущества и недостатки.

- Диски обеспечивают высокую скорость работы, но стоят довольно дорого.
- Ленты также отличаются хорошей скоростью, но ими сложнее управлять.

  

  Лента считается менее надежным носителем, чем диск, поскольку ее легко повредить при использовании. Тем не менее ленты обходятся гораздо дешевле остальных носителей, особенно, если речь идет о больших объемах данных.
- Облако отлично подходит для удаленных пользовательских устройств и малых серверов.

  Очень эффективно создавать резервные копии локально и копировать их в облако. При этом локальные копии подойдут для любого восстановления, кроме аварийного, а дополнительные копии будут лежать в удаленном хранилище на случай форс-мажорных обстоятельств.

Представленный метод двойной защиты очень экономичен и соответствует правилу 3-2-1.

Убедитесь, что ваш поставщик облачного сервиса предоставляет услугу начального сохранения. У вас должна быть возможность отправлять жесткие диски в облачное хранилище для первичного копирования, а также получать необходимые диски для масштабного восстановления.

Какой тип носителя вы выберете? Наиболее частый ответ — «все вышеперечисленные». Все три типа носителей приемлемы по стоимости и объему хранилища. Главное – правильно использовать их возможности для нужд вашей компании.

Помните, что рекомендуется использовать два типа носителей в соответствии с правилом 3-2-1 (см. введение к этой главе). Если вам не нужно копировать петабайты данных, а бюджет не слишком ограничен, пользуйтесь локальными дисками и удаленным облачным хранилищем. Для больших объемов данных лучше воспользоваться локальным ленточным хранилищем: оно будет экономичнее дисков.

В следующих разделах мы подробно расскажем о каждом из трех типов носителей.

Диски

В качестве устройств для резервного копирования диски имеют немало преимуществ:

- они надежны и энергонезависимы.
- данные на дисках сохраняются даже при отключении питания.
- диски отличаются высокой скоростью работы и обеспечивают самое быстрое восстановление.

6 ТБ — много ли это?

Большое влияние на ИТ-рынок оказало неуклонное падение стоимости вычислительных ресурсов. Только представьте, что в 1980 году один гигабайт дискового пространства стоил 200 000 долларов, а сегодня – в среднем 4 цента. Вся вычислительная мощность, которая использовалась во время Второй мировой войны, сейчас могла бы уместиться в микросхеме музыкальной открытки, а общая вычислительная мощность для запуска корабля «Аполлон» на Луну легко поместится в вашем смартфоне.

Так сколько же данных будет содержать самый большой современный диск емкостью 6 ТБ? В одном гигабайте легко помещается 100 000 сообщений электронной почты. 6 ТБ = 6000 ГБ, то есть 6 ТБ = 6 000 000 000 сообщений.

Емкость современных дисков может достигать шести терабайт (см. комментарий), что сказывается на их производительности. Однако эта проблема редко заявляет о себе при использовании дисков только для резервного копирования. Рекомендуем вам приобретать диски с наименьшей ценой за гигабайт. *Советы по подсчету необходимого количества дисков для хранения см. в разделе «Политика хранения».*

Если вы собираетесь перевозить диски или кассеты с лентами (например, во внешнее хранилище), сделайте две копии каждого носителя. Это необходимо на случай потери или повреждения при транспортировке.

В последнее время для резервного копирования используются и твердотельные накопители (SSD). Они работают еще быстрее, чем обычные диски, и гораздо более надежны. Однако у SSD есть особенности жизненного цикла, которые программа резервного копирования должна учитывать. Они связаны с методом записи данных на накопитель. Поинтересуйтесь у поставщиков ПО для копирования, имеют ли их программы специальные функции записи на SSD. Если нет, ваше ПО будет давать сбои.

Ленты

Вопреки распространенному мнению, ленты не уходят в прошлое: напротив, производители из года в год поставляют надежные ленточные носители, которые отличаются низкой ценой за гигабайт и повышенной емкостью. Текущий стандарт LTO-6 позволяет хранить 5,6 ТБ на одной кассете. На подходе новые стандарты LTO-7 (16 ТБ) и LTO-8 (32 ТБ). В обычную 19-дюймовую стойку помещается 560 слотов с подключенными лентами общем емкостью 17 петабайт. Это больше, чем может потребоваться любой компании, если не брать в расчет самые крупные центры обработки данных.

Если вы отправляете ленты на хранение в другое место, делайте копию каждой ленты на случай повреждения в процессе перевозки.

Облако

Самое большое преимущество облачного хранилища — удобство. При хранении в облаке не нужно беспокоиться о перевозке носителей и делать копии на случай повреждения в дороге, как это приходится делать для дисков и лент. Однако у облачных сервисов есть и недостатки:

- **Безопасность.** Проверьте уровень безопасности облачного сервиса, который планируете использовать в качестве хранилища. Задайте поставщикам сервиса несколько вопросов:

- Защищено ли их хранилище от пожаров?
- Есть ли в нем аварийные генераторы и резервные точки подключения к сети?
- Кем выполняется фактическое резервное копирование?
- Шифруются ли данные в хранилище?
- Кто имеет доступ к данным в центре хранения?
- Есть ли в хранилище персонал, который работает круглосуточно, или оно полностью автоматизировано?

- **Цена.** Вопрос стоимости облачного хранения неоднозначен. Многие поставщики берут плату и за использование места в хранилище, и за передачу данных.

  Кроме того, вы можете не увидеть значительной экономии, если резервное копирование в облако не позволит вам сократить штат. Вам все равно будут нужны сотрудники, чтобы управлять хранилищем, планировать его емкость, создавать расписание резервного копирования, отслеживать статус операций и контролировать доступ к данным.

- **Пропускная способность сети.** Нужно определить пропускную способность сети: она не должна отрицательно сказываться на директивном времени восстановления (RTO, Recovery Time Objective). *См. раздел «Восстановление в облаке» далее в этой главе.* Необходимая пропускная способность для ежедневного резервного копирования будет меньше, чем для полного восстановления.

Кроме перечисленных слабых мест, облачные и сетевые технологии имеют множество преимуществ:

- Поставщик облачного сервиса обеспечивает надежное сетевое подключение, так что вы сможете иметь доступ к данным отовсюду.
- Работать по сети очень удобно.
- Вам не нужно будет беспокоиться о сохранности и проверке носителей. Поставщик обеспечивает их защиту и часто делает избыточные копии данных, хотя стоит отметить, что у некоторых компаний облачное хранение с высокой доступностью стоит дороже.
- Поставщик облачного сервиса позволит вам быстро увеличивать или уменьшать объем хранилища.

Выбор внешнего хранилища

Согласно правилу 3-2-1 (*см. введение к этой главе*) необходимо иметь три копии данных: рабочую систему, локальные резервные копии и копии во внешнем хранилище. Диски или ленты можно перевезти во внешнее хранилище или обратиться к поставщику, который сделает это за вас. Кроме того, данные могут быть переданы по беспроводной сети для записи на сетевое устройство. Остановимся на этом подробнее.

Если вы собираетесь хранить один набор резервных копий на рабочих машинах, а второй — во внешнем хранилище, решите, на каком расстоянии оно должно находиться. Большинство компаний предпочитают, чтобы дорога до внешнего хранилища и обратно занимала не более восьми часов. Это разумное расстояние. Если в вашей местности нередки стихийные бедствия (землетрясения, наводнения, ураганы), то, возможно, вы предпочтете хранить резервные копии дальше.

Сетевое хранилище

Прежде, чем использовать сеть в качестве второго хранилища, вам стоит узнать у поставщика услуги, как обеспечивается безопасность данных и какова пропускная способность сети. После этого нужно определить, какая часть ваших данных будет регулярно изменяться. Производственная норма — 5%; но, конечно, объем изменений может быть большим или меньшим. Например, базы данных изменяются часто, а коды приложений — нет.

Обратите внимание и на скорость. Допустим, у вас небольшая компания с десятью сотрудниками. На каждого из них приходится по 5 ГБ данных. Также у вас есть два сервера по 10 ГБ, то есть всего вам понадобится 70 ГБ в день и 1,4 ТБ при начальном резервном копировании. При условии, что скорость передачи данных по сети составляет 100 Мбит/с, ежедневное инкрементное резервное копирование будет занимать у вас 90 минут. И это, не считая дополнительной нагрузки на сеть и задержек при маршрутизации.

Большое преимущество может дать сжатие. Если сжать данные на половину их объема, то и передать по сети нужно будет лишь половину, что значительно повысит скорость. *Подробнее об этом читайте в разделе «Сжатие и дедупликация данных» далее в этой главе.*

Теневой сайт

Если вам не нужны два рабочих сайта или вы не можете себе их позволить, возможно, вас заинтересует создание *теневого сайта*. Обычно это удаленное хранилище с минимальным количеством оборудования. Как правило, все резервные копии отправляются по сети на расположенные там устройства хранения. Периодически теневой сайт компании поднимается и запускается, чтобы проверить работу плана аварийного восстановления.

Резервное копирование в облако

Резервное копирование в облака стремительно набирает популярность. К нему прибегают компании, которые хотят иметь локальные центры обработки данных, используя облако для временных нужд и аварийного восстановления. К тому же сейчас стало значительно проще использовать облако в качестве второго сайта. В нем можно сохранять резервную копию сайта и при необходимости восстанавливать ее на сервер этого же облака.

Восстановление в облаке

Прежде, чем прибегать к сетевому/облачному резервному копированию, убедитесь, что пропускная способность сети согласуется с директивным временем восстановления (RTO). Так, если RTO равно двум часам, потерянные данные явно не должны восстанавливаться из облака дольше.

Произведем небольшой подсчет. Если значение RPO (см. главу 2) составляет четыре часа, а RTO — два часа, вы сможете продолжить работу через два часа после сбоя. При этом потеряются данные за последние четыре часа или за меньшее время – в зависимости от последней точки восстановления. Чтобы через два часа продолжить работу со всеми данными, значения RPO и RTO вместе должны составлять не более двух часов.

RTO обычно применяется к серьезным сбоям подсистемы или целой системы. Например, для отдела приема заказов значение RTO может составлять всего 5 минут, а для отдела расчета зарплаты — два дня.

Первое резервное копирование в облако может занять очень много времени, поскольку по сети будет передаваться весь объем данных. Чтобы сократить это время, поставщик облачного сервиса может отправить вам диски для начального сохранения. Если вам потребуется полное восстановление, провайдер также может отправить необходимые данные на дисках.

Публичное или частное облако

Принимая решение использовать общедоступный облачный сервис, нужно тщательно взвесить все доводы за и против. Многие поставщики решений для резервного копирования, а также крупные облачные сервисы предлагают облачные хранилища, оптимизированные для резервных копий. Серьезное преимущество такого хранилища – возможность легко увеличивать объем.

Система оплаты в общедоступных облачных сервисах может быть довольно запутанной. Некоторые поставщики берут годовую плату за определенный объем хранения, другие — взимают ее ежемесячно. В случае ежемесячной платы вам придется платить за данные, переданные из хранилища в интернет. Также может устанавливаться дополнительный тариф, например, за удаление данных. Выбирая хранилище, обязательно проверьте уровень его безопасности..

Сжатие и дедупликация данных

Сжатие подразумевает уменьшение размера файлов. Сжатие выполняется с помощью различных алгоритмов, которые заменяют повторяющуюся информацию сокращениями. Этот метод эффективен, когда данные содержат большое число предсказуемых элементов. Например, если компания называется Acronis, название будет часто появляться в корпоративных текстах. Программа зарегистрирует этот факт и создаст для него сокращение. Сжатие часто используется для локальных резервных копий и работы хранилищ.

Такие типы данных, как изображения или видео, уже сжаты, поэтому дополнительно уменьшить их в резервной копии не получится. Зашифрованные данные по сути своей непредсказуемы, поэтому их тоже нельзя сжать. Более того, если вы *можете* сжать зашифрованные данные, это повод задуматься о замене системы шифрования.

Дедупликация (или *устранение дублирования*) работает аналогично сжатию. Например, вам необходимо создать 1000 резервных копий образа системы стандартных корпоративных ноутбуков. В этих копиях все время будут повторяться одни и те же файлы ОС, и большое число дубликатов займет много лишнего места. С помощью дедупликации можно сохранить одну копию общих данных, на которую в каждой резервной копии будет сделан специальный указатель. Дублированные данные могут содержать тысячи символов, а указатель — всего 20, так что экономия места будет значительной.

Можно использовать несколько методов дедупликации. Сперва применяется дедупликация на лету: она сокращает объем данных, записываемых в архив резервных копий. Затем можно выполнить постобработку для дедупликации готовых архивов.

Если вы хотите с помощью дедупликации сэкономить время и место в хранилище, проверьте, как этот метод будет работать с вашими данными. Сравните полученный результат с другими вариантами. Не исключено, что вам лучше просто сократить объем создаваемых дубликатов.

Расчет стоимости

Рассчитать точную стоимость хранения резервных копий сложно, но в этом вам могут несколько общих правил:

- Средняя стоимость диска составляет сегодня 3–4 цента за 1ГБ неформатированного пространства, а стоимость ленты — примерно 1 цент за 1ГБ.
- Поставщики облачных сервисов взимают ежемесячную абонентскую оплату, передача данных также оплачивается. На момент написания этого текста стоимость сервиса Amazon.com составляет 2–3 цента в месяц за 1ГБ в хранилище. К этому нужно добавить 12 центов за 1ГБ сетевого трафика в месяц за данные, которые передаются из хранилища Amazon в интернет.
- Цены на облачные сервисы включают стоимость обслуживания помещений, систем кондиционирования, контроллеров и стоек, а также счета за электричество. Посчитайте, во сколько это обойдется в вашем собственном локальном хранилище. Общая стоимость систем жизнеобеспечения может быть в 5–20 раз выше стоимости носителей.

Сегодня запись на ленты является самым дешевым методом резервного копирования, диски требуют больше затрат, а самым дорогим способом хранения будет облако. Однако по общим расходам облако нередко оказывается выгоднее. Можно начать с самого недорогого облачного варианта и доплачивать за место по мере надобности. В случае с дисками и лентами придется сразу приобрести большую часть инфраструктуры.

Убедитесь, что ваша программа резервного копирования работает с дисками, лентами и облачным хранилищем, а также с физическими, виртуальными и облачными системами. Затем выберите для себя самое экономичное решение в соответствии с правилом 3-2-1. Если ваша система копирования поддерживает работу со всеми популярными типами носителей, вы сможете легко корректировать стратегию их использования.

Глава 4

Восстановление данных

В этой главе

- Как распознать потерю данных
- Как запустить план восстановления
- Стремитесь к простоте

Восстановление данных может потребоваться в самых разных случаях. Наиболее частый — ошибка пользователя: к примеру, случайное удаление важного письма или перезапись старой версии файла поверх новой. Обратиться к резервной копии могут заставить вирусы и вредоносные программы, саботаж со стороны недовольных сотрудников, неполадки с дисками, контроллерами и сетевыми устройствами, программные ошибки в приложениях и операционных системах. Иногда файлы теряются просто потому, что никто не помнит, куда их сохранили.

Восстановить данные — значит, вернуть их на место, будь то потерянный номер телефона или данные целой компании, уничтоженные стихийным бедствием.

В этой главе мы рассмотрим, как создать план восстановления данных, который поможет вам в экстренном случае.

Если вы читаете эту главу, потому что уже потеряли все данные, а резервной копии не сохранилось, вот вам пара советов. Обратитесь к специалистам, которые попробуют извлечь информацию в случае, если проблема связана со сбоем электроники внутри диска. Главное, чтобы сам диск и головки не были повреждены под действием высокой температуры, или из-за попадания внутрь воды и пыли. Кроме этого, в сети можно найти программы, которые помогут восстановить данные, даже если диск отформатирован. Но надо иметь в виду: восстановить информацию не получится, если она стерта специальными средствами, диск зашифрован, и вы не знаете пароля, или если вы достаточно долго после случайного удаления записывали на диск новые данные.

Как распознать потерю данных

Потеря данных не всегда очевидна. Иногда ее можно спутать с аппаратным сбоем, программной ошибкой, нехваткой памяти или места на диске. Вот несколько возможных сценариев:

- **После серьезного сбоя система загружается, но приложения не работают.** В этом случае просмотрите журналы приложений и сообщения об ошибках или сверьтесь со средствами системного мониторинга. Скорее всего, возобновить работу системы нужно очень быстро. А если проблемы возникли сразу с несколькими приложениями, полное восстановление может занять много времени. Поэтому прежде, чем его запускать, определите причину неполадки. Возможно, на работу приложений влияет недавнее обновление системы, или повреждены данные, которые используют эти приложения.

  

  Иногда все-таки проще восстановить систему на виртуальную машину (ВМ) или подключить резервную копию, как виртуальный диск, и провести быстрое сравнение, – чем долго диагностировать проблему. Но даже в таком случае после возобновления работы выясните причину сбоя: он вполне может повториться.

- **После серьезного сбоя система и приложения работают, но появляются сообщения о поврежденных данных.** Вы можете усомниться в том, что данные и вправду потеряны. Поскольку система работает, можно выполнить несколько запросов и посмотреть на результат. Например, вы заметили, что сообщения об ошибке приходятся на определенный период времени или связаны только с одним типом операций: если это так, не исключено, что повреждена таблица в базе данных. Как и в первом случае, самым простым выходом может быть полное восстановление, но при условии, что у вас есть актуальная резервная копия.

  

  Распространенная ошибка – попытка исправить неполадку. Нередко на это уходит больше времени, чем на восстановление системы до последней рабочей точки.

Рано или поздно вы столкнетесь с потерей данных. Вопрос лишь в том, когда это произойдет. Как правило, потери информации незначительны и носят локальный характер, однако они случаются намного чаще, чем кажется. По статистике, в небольших компаниях восстановление данных требуется один-два раза в неделю. Сотрудники случайно удаляют важную переписку или не могут найти презентацию, сделанную полгода назад. Если восстановить данные невозможно, приходится переделывать многочасовую работу или принимать решение без всей необходимой информации.

Кроме этих рутинных случаев, вся система может быть повреждена во время обновления. С проверенным планом восстановления, эта проблема вполне решаема. Просто помните, что с обновлениями связано больше рисков, чем обычно думают, и будьте готовы, если нужно, запустить полное восстановления системы. Главное – не растеряться и иметь четкий план.

Лучший совет для быстрого восстановления - чаще устраивайте себе тренировки. Практика гарантирует вам знание процесса, наличие необходимых материалов и программ, и то, что план резервного копирования сработает, как надо.

Будьте осторожны в обращении с резервными копиями. Иногда система повреждает диски, и ИТ-специалист, сославшись на то, что нет времени на восстановление, загружает машину из резервного образа. Однако спустя несколько минут резервный образ может постичь та же участь. В других случаях администратор подключает резервную копию и решает перед восстановлением на всякий случай переформатировать системный диск; при этом он так нервничает, что по ошибке форматирует диск с копией.

Не усложняйте

Избегайте лишних сложностей. Правильней выбрать решение от одного поставщика; при условии, что оно обеспечит резервное копирование и восстановление физических, виртуальных и облачных хранилищ в системах Windows и Linux, а также фрагментарное восстановление приложений — все с помощью резервной копии образа. Это гораздо удобнее, чем выбор одного продукта для восстановления Microsoft Exchange, другого — для SQL, третьего — для восстановления на «голое железо» и т. д. Работа со средствами от нескольких поставщиков может быть слишком сложной и запутанной, к тому же вполне реальны проблемы с совместимостью. Наконец, вам придется гораздо чаще обновляться и менять процедуры восстановления.

Постарайтесь сделать вашу среду резервного копирования как можно полнее, но и как можно проще.

Как запустить план восстановления

Будем надеяться, что у вас уже разработан набор процедур восстановления, которые вы оттачиваете на практике. Если же нет, следуйте этим пунктам:

1. **Загрузите хост-систему, которую необходимо ввести в действие с помощью программы резервного копирования.**
2. **Восстановите гипервизор – и, по возможности, виртуальные машины – на диск, расположенный на хосте.**
3. **Загрузите хост.**
4. **Запустите виртуальные машины или же сначала восстановите их из другого набора резервных копий, а затем запустите.**

Если вы уже практиковались, то быстро и успешно со всем справитесь.

Некоторые программы резервного копирования могут выводить на печать описание процедуры восстановления. Легко забыть, какие файлы содержатся на тех или иных дисках, – особенно, при нервном напряжении и в спешке. Распечатанные инструкции не дадут вам ошибиться.

Неплохо будет назначить ответственного за восстановление, который при случае выполнит все нужные шаги. Слишком много людей и действий приведут к тому, что восстановление, скорее всего, кончится неудачей. Кроме этого, для копирования стоит выбирать продукт с функцией активного восстановления: это позволит запустить систему, как только будет воссоздано достаточно данных. После этого процесс завершится в фоновом режиме при уже работающей системе.

Глава 5

Управление резервным копированием

В этой главе

- Будьте в курсе новых технологий
- Что и когда следует копировать
- Планирование работы и выполнение плана

Секрет успешного резервного копирования и восстановления – правильные привычки и аккуратность в работе. В аварийной ситуации вы можете стать последней надеждой для своей компании. Поэтому учитесь и практикуйтесь, чтобы справиться с проблемами, когда они появятся.

Ваша работа включает две похожие задачи:

- Создать хороший план резервного копирования и отслеживать его исполнение.
- Обеспечить оптимальный план восстановления и проверять его эффективность.

В этой главе мы расскажем, как это сделать.

Будьте в курсе новых возможностей резервного копирования

Прежде всего, следите за обновлениями продуктов для резервного копирования. Также не забывайте про новые версии оборудования и ПО, которые используются в вашей компании. Эта задача сама по себе предполагает много работы. В новых версиях появляются дополнительные функции, да и сами методы использования информационных технологий постоянно меняются.

Так, виртуализация когда-то представляла собой лишь малую часть системы, позволявшую объединить слабо загруженные серверы. Сегодня это один из основных компонентов центров обработки данных, благодаря которому ресурсы расходуются гораздо эффективней. Одно только развитие виртуализации привело к появлению множества новых функций в решениях для резервного копирования. В последнее время на первый план выходят программно-определяемые хранилища, интернет вещей, а также слияние разработки и эксплуатации ПО (DevOps). Все эти технологии бросают программам для резервного копирования новый вызов.

Разработайте долгосрочную стратегию резервного копирования, которая будет соответствовать общей ИТ-стратегии вашей компании. В ИТ-стратегию можно включить расширение использования ПО как услуги (SaaS), развитие виртуализации или территориальный рост. Учтите, что избранные методы резервного копирования должны будут работать и в новой ИТ-структуре.

Настройка окна резервного копирования

После того, как вы вошли в курс всех новинок, следующая и, наверное, самая сложная задача — определить значение директивной точки восстановления (RPO) так, чтобы она сочеталась с окном резервного копирования и директивным временем восстановления (RTO). *Подробнее об RPO можно узнать в главе 2, а об RTO — в главе 3.* Для определения RPO необходимо выявить:

- основные приложения, требующие защиты;
- объем данных (текущий и планируемый), который используют эти приложения;
- значения RPO и RTO для этих приложений.

Собрав эту информацию, вы поймете, сколько времени нужно отвести под резервное копирование. К сожалению, во время копирования нередко возникают паузы, а работа приложений замедляется. Эти проблемы можно решить, передвинув копирование на периоды наименьшей загрузки. Однако учтите, что во время наибольшей активности данные изменяются чаще всего и поэтому сильней нуждаются в защите.

Не существует однозначного ответа на вопрос о том, сколько времени должно занимать резервное копирование. Главное – обеспечить достаточное количество вычислительных ресурсов для одновременного хода копирования и рабочих операций.

Создание и проверка плана резервного копирования

Если вам нужен быстрый откат системы практически на любой момент времени и долгое хранение резервных копий, то придется постараться. Вот несколько полезных идей:

- Гибридное локальное и облачное хранилище (см. главу 3). Поможет свести к минимуму объем данных, перемещаемых во второе хранилище.
- Политика хранения «Ханойская башня» (ToH) (см. главу 3). Обеспечит частые точки восстановления. «Ханойская башня» гарантирует наличие и недавних, и более старых точек на случай неочевидных повреждений, которые присутствовали в системе уже давно.
- Дедупликация и сжатие. Значительно уменьшат объем, занимаемый данными в хранилище (см. главу 3).
- Резервные копии образов и грамотное использование инкрементного резервного копирования и консолидации. Помогут уменьшить необходимый объем хранилища, не жертвуя показателями RTO (см. главу 2).

Не забывайте о едином плане резервного копирования. Поставщик вашего решения должен предоставлять общую консоль управления. С ее помощью вы настроите эталонный план копирования для каждой системы, установите этот план на одной из них, будете отслеживать ход его выполнения и проверять его на наличие ошибок.

Простота или сложность

План резервного копирования может быть очень простым; например, полная резервная копия всех данных создается ежедневно в полночь. Однако нередки и сложные планы – как в следующем варианте:

> Для системы приема заказов: полное резервное копирование каждую неделю и инкрементное – каждый час. Для системы управления запасами: резервное копирование только базы данных каждые 15 минут. Для систем управления производством: полное резервное копирование образа каждые четыре часа. Для всех конечных устройств пользователей: полное резервное копирование с дедупликацией в источнике раз в месяц и инкрементное резервное копирование с шифрованием и сжатием каталогов пользователей – каждые 12 часов. Распределение по времени произвольное.

Чем сложнее корпоративные требования к RPO и RTO, тем сложнее будет план резервного копирования. Поэтому так важно использовать решения наименьшего числа производителей.

Настройка окон резервного копирования

Окно резервного копирования — это время, на которое система может останавливаться или снижать скорость работы для создания резервной копии. Если ваше предприятие работает по две смены в день, окно резервного копирования может составлять восемь часов. Но если производство идет круглосуточно, копирование, скорее всего, придется выполнять при работающей системе.

Технологии создания резервных копий постоянно совершенствуются, но реализовать процесс с нулевым окном пока нелегко. Иногда вопрос удается решить через создание нескольких коротких окон копирования для разных рабочих нагрузок. В других случаях оптимизировать время копирования и автоматизировать процесс помогает мощная централизованная консоль управления.

Поставщики лучших решений предлагают консоль управления, которая поможет составить план резервного копирования и настроить для него правильный график. Консоль нужна, чтобы создание копий не шло одновременно и не потребляло слишком много ресурсов. Когда появляется новый сервер или рабочая нагрузка, их можно быстро добавить в план. Составляя план копирования, нужно выделить правильное количество хранилищ и архивов, чтобы эффективно использовать дедупликацию и обеспечить оптимальное распределение нагрузки по устройствам.

Проверка плана на ошибки

После того, как план резервного копирования заработает, проверяйте его на наличие ошибок. Проверка позволит убедиться, что все резервные копии созданы успешно, или, если это не так, поможет найти причину сбоев. Самая распространенная причина – нехватка места на диске. На втором месте идут проблемы с сетевым подключением.

Текущее наблюдение за планом

Когда план резервного копирования составлен, ежедневные резервные копии создаются, управление хранилищем настроено и сетевое подключение установлено, у вас остаются две ключевые задачи:

- **Отслеживать изменения.** Гибкие возможности современных виртуальных и облачных центров обработки данных позволяют легко распределять рабочие нагрузки. При этом новые виртуальные машины (ВМ) могут появляться в любой момент. Грамотное управление резервным копированием подразумевает, что копии этих ВМ создаются с учетом существующих файловых ограничений и условий синхронизации.
- **Вести списки.** Ведите учетный список систем, дисков и архивов, чтобы гарантировать создание нужных резервных копий.

Глава 6

Десять вещей, которые нужно знать о резервном копировании

В этой главе

- Определение стоимости
- Расстановка приоритетов
- Что и когда следует делать

Когда создание резервных копий идет своим чередом, а процедура восстановления отработана на практике, даже звонок в 2 часа ночи вас не смутит. Вы будете уверены в себе и готовы действовать. В этой главе перечислены десять фактов, которые нужно знать о резервном копировании и восстановлении, чтобы облегчить себе работу.

Ценность ваших данных

Корпоративные данные существуют в самых разных формах. Некоторые изменяются очень быстро, другие — постепенно. Одни связаны с продажами, другие — с продуктами и услугами, третьи — с финансовой отчетностью, маркетингом или кадрами. Когда известно, насколько важен тот или иной тип данных и как часто они меняются, можно определить для них оптимальное значение RPO.

Обычно значение RPO вычисляется по рабочим нагрузкам или приложениям. Дополнительные сведения по RPO см. в главе 2.

Стоимость времени простоя

Порой цену простоя рассчитать легко. Если не работает производство, достаточно сложить стоимость бездействия рабочих и стоимость непроизведенной продукции. При сбое системы бронирования авиабилетов ситуация будет куда сложней. Если

система не продает билеты, авиакомпания может потерять и существующих, и потенциальных клиентов, а кроме этого еще и репутацию. Все это имеет свою ценность, но высчитать ее с точностью невозможно.

Конечно, стоимость простоев зависит от типа бизнеса, но в любом случае ценность имеют как данные, так и бесперебойная работа. Именно поэтому так важна страховка – хорошо настроенный процесс резервного копирования.

В недавнем *опросе об аварийном восстановлении*, проведенном компанией IDC при поддержке Acronis (май 2014 г.), более 90% компаний сообщили, что стоимость простоев для них превышает 20 000 долларов в час. При этом почти половина опрошенных теряет на простое более 60 000 долларов в час.

Приоритет рабочих процессов

Если все данные потеряны целиком, нужно расставить приоритеты восстановления. Обратите внимание на следующие моменты:

- Очередность, с которой будут возобновляться рабочие процессы.
- Для каких рабочих процессов необходима избыточность и отказоустойчивость.
- Какие рабочие процессы могут подождать несколько дней, а какие — нет.
- Какие рабочие процессы можно остановить, чтобы перенаправить ресурсы туда, где произошел сбой.

Где хранятся резервные копии

Для хранения копий рекомендуется применять правило 3-2-1: три копии данных, два типа носителей, одна копия в удаленном хранилище (см. главу 3). В идеале у вас должна быть рабочая система, не подключенная локальная копия и еще одна копия во внешнем хранилище. Так будет надежней всего.

Как долго следует хранить резервные копии

Место в хранилище ограничено, поэтому в какой-то момент нужно будет удалить часть резервных копий в соответствии с принятой в компании политикой хранения (см. главу 3). Обратите внимание на три аспекта:

- **Правовые требования.** Некоторые компании обязаны хранить часть данных в течение определенного времени. Это может быть личная информация (в регулируемых отраслях) или условия договора между компанией и клиентами.
- **Как часто используются файлы.** Допустим, вы ведете переписку и обмениваетесь файлами с клиентом в течение трех месяцев, после чего работа завершается. В этом случае достаточно хранить резервные копии 4–6 месяцев.
- **Версии.** Файлы могут иметь множество редакций, и не всегда важно хранить каждую из них. После завершения проекта в резервной копии сохраняется итоговый вариант, а промежуточные, как правило, больше не нужны.

Какие средства восстановления использовать

Для успешного восстановления нужны: оборудование, резервные копии операционной системы (ОС) вместе со всеми исправлениями и обновлениями, приложения, параметры конфигурации и, разумеется, сами данные, которые используются приложениями. Если создаются полные резервные копии образов, все системные данные будут содержаться в образе, но при резервном копировании на уровне файлов систему придется отдельно собирать и обновлять.

Подробные сведения о плане резервного копирования

Процедуры восстановления стоит документировать по нескольким причинам:

- Если генеральный директор случайно удалил нужный файл, он должен знать, кому звонить посреди ночи.
- Сотрудник, которому звонит директор, должен знать, как восстановить файл.
- В случае более серьезного сбоя, техническому персоналу необходимо знать, где находится резервная копия, какие серверы следует восстановить и как это сделать.

Какие данные исключаются из резервной копии

Когда места начинает не хватать, администраторы идут на хитрости и исключают ненужные данные. Как правило, этот факт обнаруживается слишком поздно.

Допустимо исключать файлы, которые легко воссоздать. Если же список исключаемых из резервной копии файлов слишком длинный, лучше убедиться, что экономия нескольких долларов на дисковом пространстве не приведет к многодневному восстановлению.

Как (и насколько тщательно) следует проверять резервные копии

Если в компании имеется хороший план для тестирования производительности, его можно использовать, чтобы проверить правильность восстановления из резервных копий. При наличии запасных серверов или свободного места на виртуальном хосте неплохо будет организовать автоматическое тестирование. Минимальная проверка включает восстановление из резервных копий, проверку дисков и сравнение размеров всех файлов.

Как формулировать вопросы по резервному копированию

Для ответа на вопрос по резервному копированию следует помнить про восстановление. Не спрашивайте себя, какой носитель лучше и какая политика хранения оптимальней; задайте себе один из таких вопросов:

- Какой носитель обеспечит самое быстрое восстановление?
- Какой носитель будет самым надежным?
- Позволит ли схема «дед-отец-сын» восстановить данные из старых резервных копий? (Политика «дед-отец-сын» (GFS) описывается в главе 3).
- Какая политика хранения позволит восстановить данные быстрее всего?

Не стоит оптимизировать резервное копирование, если вы не уверены, что это не вызовет проблемы при восстановлении.

Acronis

Резервное копирование и управление хранением данных для дома и бизнеса

Продукты и решения для любых бизнес-сред

Acronis предоставляет лучшую защиту данных нового поколения для виртуальных, физических, мобильных и облачных сред

Компания предлагает самые удобные и комплексные решения для резервного копирования, аварийного восстановления данных и безопасного доступа, основанные на технологии **AnyData Engine**. Решения Acronis обладают полным набором технологических преимуществ:

Технология резервного копирования Acronis охватывает *любые* типы данных

Быстрый процесс аварийного восстановления поможет возобновить работу за считанные минуты

Гибкое восстановление данных: возможность восстановления как отдельных файлов, так и целых серверов

Поддержка резервного копирования в различные типы хранилищ позволяет сохранять резервные копии везде, включая Acronis Cloud

Специализированные средства развертывания системы позволяют организовать ИТ-инфраструктуру любой сложности за несколько простых шагов

Средства интеллектуального управления дисками упрощают ИТ-задачи и повышают производительность системы

Исключительная простота использования ПО практически не требует от пользователей специальных навыков и знаний

Централизованное управление и простой процесс генерации отчетов с помощью универсальной и удобной консоли

Загрузите бесплатную пробную версию ПО Acronis Backup and Recovery сегодня

Посетите www.acronis.com/ru-ru/backup/free-trials

Acronis

Больше никаких потерь файлов!

Настало время менять способы защиты данных. Сегодня данные хранятся на физических серверах, в настольных компьютерах, ноутбуках, виртуальных машинах и облаках. С появлением новых технологий растет необходимость в улучшенных методах защиты информации и в более быстром восстановлении после аварий с потерей данных.

- ***Современное резервное копирование и восстановление:*** ***средства защиты данных нового поколения***
- ***Создание плана резервного копирования:*** ***ключевые моменты и рекомендации***
- ***Виртуальные, физические и облачные среды:*** ***защита любой среды***
- ***Восстановление любых данных:*** ***файлы, приложения и целые системы***

Открыв эту книгу, вы найдете информацию:

- **Об основах защиты данных**
- **Как подготовить данные для резервного копирования**
- **Как безопасно хранить резервные копии**
- **О способах восстановления данных**

Джоэл Берман (Joel Berman) работает в сфере ИТ более 40 лет. Он обеспечивал надежность ИТ-инфраструктуры крупнейших финансовых и телекоммуникационных компаний мира.

WILEY

ISBN 978-1-119-10185-7
Не для перепродажи