РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

Дисциплина: Информационная безопасность

ДОКЛАД

на тему

«Системы резервного копирования»

Выполнил

Студент группы НКНбд-01-19

Топонен Никита Андреевич

Москва 2022 г.

Оглавление

1. Что такое резервное копирование?

1.1 Определение

Резервное копирование данных — процесс создания копии данных на носителе, предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения. Кроме того, система резервного копирования — это один из необходимых методов обеспечения непрерывности бизнеса.

1.2 Важность резервного копирования

Важность регулярного резервного копирования или бэкапа (от англ. *backup*) и хранения резервных копий критически важных данных можно проиллюстрировать на простом примере. После атак вирусов-шифровальщиков WannaCry и NotPetya быстрее всего к работе возвращались те организации, которые просто восстановили резервные копии своих систем. То есть такие системы очень важны в функционировании организаций, хранящих данные, которые подвержены риску бесследного исчезновения, так как в таком случае возможно достаточно быстро и эффективно восстановить работоспособность в короткие сроки.

2. Система резервного копирования

Система резервного копирования - совокупность программного и аппаратного обеспечения, выполняющее задачу создания копии данных на носителе, предназначенном для восстановления информации в оригинальном месте их расположения в случае их повреждения или разрушения.

Система резервного копирования (СРК) определяется:

- Политикой резервного копирования. Политика задаёт основные цели и задачи резервного копирования, требования к нему, исходя из списка угроз для каждой резервируемой системы, а также обосновывает его необходимость.
- Регламентом резервного копирования, определяемого политикой. Регламент описывает алгоритмы резервного копирования и восстановления, ответственных за резервное копирование, условия хранения резервных копий и прочее.
- Инструментальной реализацией. Собственно, программное и аппаратное обеспечение.

Регулярный процесс резервного копирования делится на следующие основные части:

- Периодический запуск копирования.
- Запуск восстановления по требованию.
- Тестирование процесса копирования.

3. Архитектура и работа системы резервного копирования

Централизованная система резервного копирования имеет многоуровневую архитектуру, в которую входят:

- сервер управления резервным копированием, способный также совмещать функции сервера копирования данных;
- один или несколько серверов копирования данных, к которым подключены устройства резервного копирования;
- компьютеры-клиенты с установленными на них программами-агентами резервного копирования;
- консоль администратора системы резервного копирования.

Администратор системы ведет список компьютеров-клиентов резервного копирования, устройств записи и носителей хранения резервных данных, а также составляет расписание резервного копирования. Вся эта информация содержится в специальной базе, которая хранится на сервере управления резервным копированием.

В соответствии с расписанием или по команде оператора сервер управления дает команду программе-агенту, установленной на компьютере-клиенте, начать резервное копирование данных в соответствии с выбранной политикой. Программа-агент собирает и передает данные, подлежащие резервированию, на сервер копирования, указанный ей сервером управления.

Сервер копирования сохраняет полученные данные на подключенное к нему устройство хранения данных. Информация о процессе (какие файлы копировались, на какие носители осуществлялось копирование и т. п.) сохраняется в базе сервера управления. Эта информация позволяет найти местоположение сохраненных данных при необходимости их восстановления на компьютере-клиенте.

Чтобы система резервного копирования сохраняла непротиворечивые данные компьютера-клиента, они не должны подвергаться изменениям в процессе их сбора и копирования программой-агентом. Для этого приложения компьютера-клиента должны завершить все транзакции, сохранить содержимое кэш-памяти на диск и приостановить свою работу. Этот процесс инициируется по команде программы-агента, которая передается приложениям компьютера-клиента.

Поскольку система резервного копирования предназначена для восстановления данных после сбоя или аварии, созданные резервные копии необходимо проверять на предмет целостности и работоспособности. Кроме того, при построении системы резервного копирования необходимо уложиться в сокращенное «окно» резервного копирования. Вообще говоря, требование круглосуточной работы информационных систем сокращает практически до нуля доступный временной интервал остановки приложений, необходимый для

осуществления операции резервного копирования («окно» резервного копирования).

4. Классификация резервного копирования

4.1 По полноте сохраняемой информации

- Полное резервирование (*Full backup*) — создание резервного архива всех системных файлов, обычно включающего состояние системы, реестр и другую информацию, необходимую для полного восстановления рабочих станций. То есть резервируются не только файлы, но и вся информация, необходимая для работы системы.
- Добавочное резервирование (*Incremental backup*) — создание резервного архива из всех файлов, которые были модифицированы после предыдущего полного или добавочного резервирования.
- Разностное резервирование (*Differential backup*) — создание резервного архива из всех файлов, которые были изменены после предыдущего полного резервирования.
- Выборочное резервирование (*Selective backup*) — создание резервного архива только из отобранных файлов.

4.2 По способу доступа к носителю

- Оперативное резервирование (*Online backup*) — создание резервного архива на постоянно подключенном (напрямую или через сеть) носителе.
- Автономное резервирование (*Offline backup*) — хранение резервной копии на съёмном носителе, кассете или картридже, который перед использованием следует установить в привод.

5. Технологии резервного копирования

От ошибок, в результате которых изменяются или удаляются данные и в которых виноваты операционная система или человек, не защищают ни RAID, ни кластер, ни любая другая технология обеспечения отказоустойчивости. Резервное копирование — одно из оптимальных решений для таких ситуаций, так как оно позволяет хранить копии разного срока давности, например за каждый день текущей недели, двухнедельной, месячной, полугодовой и годовой давности. Возможность использовать внешние съемные носители существенно снижает затраты на хранение информации, однако для некоторых задач больше подходят альтернативные технологии.

Применение сетей хранения данных SAN (*Storage Area Network*) позволяет полностью перенести трафик резервного копирования с локальной сети на сеть хранения. Существует два варианта реализации: без загрузки локальной сети, или внесетевое копирование (LAN-free backup), и без участия сервера, или внесерверное копирование (Server-free backup).

5.1 Внесетевое копирование

При внесетевом копировании данные с диска в хранилище и обратно передаются внутри SAN. Исключение сетевого сегмента из пути резервного копирования данных позволяет избежать излишних задержек на передачу трафика через сеть IP и платы ввода-вывода. Нагрузка локальной сети падает, и резервное копирование можно проводить практически в любое время суток. Однако пересылку данных выполняет сервер, подключенный к SAN, что увеличивает нагрузку на него. Благодаря протоколу Fibre Channel с помощью одного оптического кабеля может быть организовано несколько каналов передачи данных. При этом весь объем резервируемых данных с backup-серверов хранения направляется на ленточное устройство, минуя локальную сеть. В этом случае локальная сеть необходима лишь для контроля работы самих backup-серверов со стороны главных серверов. Таким образом, только небольшой объем метаданных, которые содержат информацию о резервируемых данных, передается по локальной сети. Главные серверы отвечают в целом за политику резервного копирования данных в своем сегменте или зоне ответственности. Все backup-серверы по отношению к главному серверу являются клиентами. Считается, что рассматриваемый метод резервного копирования может максимально задействовать пиковую полосу пропускания Fibre Channel.

В качестве протокола, применяемого для передачи данных между серверами и библиотеками, могут использоваться как SCSI поверх Fibre Channel, так и IP поверх Fibre Channel, тем более что большинство FC-адаптеров и FC-концентраторов работают одновременно с обоими протоколами (IP и SCSI) на одном Fibre Channel-канале.

5.2 Внесерверное копирование

Данный тип резервного копирования представляет собой дальнейшее развитие метода внесетевого копирования (LAN-free), поскольку уменьшает количество процессоров, памяти, устройств ввода-вывода, задействованных в этом процессе. Данный процесс архивирует разделы целиком, в отличие от пофайлового архивирования, но при этом позволяет восстанавливать отдельные файлы. По определению, при вне-серверном копировании данные копируются с диска на ленту и обратно без прямого участия сервера. Поскольку для резервного копирования требуется наличие некоторого дополнительного третьего узла, полностью отвечающего за процесс копирования, то отсюда происходит и другое название этого подхода — копирование с участием третьей стороны (Third_-Party Copy, 3PC). Так, в качестве подобного оборудования может использоваться маршрутизатор хранилищ данных, который берет на себя функции, ранее выполнявшиеся сервером.

Одно из преимуществ архитектуры SAN — отсутствие жесткой привязки составляющих ее систем к каким-либо устройствам хранения данных. Это свойство и заложено в основу технологии резервного копирования без участия сервера. В данном случае к дисковому массиву может иметь прямой доступ как сервер

данных, так и устройства, принимающие участие в копировании с дисковых массивов. Резервному копированию блоков данных, относящихся к какому-либо файлу, предшествует создание некоего индекса или списка номеров принадлежащих ему блоков. Это и позволяет в дальнейшем привлечь внешние устройства для резервного копирования.

Таким образом, внесерверное копирование позволяет напрямую перемещать данные между подключенными к сети SAN дисковыми массивами и библиотеками. При этом данные перемещаются по сети SAN и не загружают ни локальную сеть, ни серверы. Такое копирование считается идеальным для корпоративных сетей, которые должны функционировать в непрерывном режиме 24 часа в сутки, 7 дней в неделю. Особенно для тех, для которых временной период, в течение которого можно выполнять резервное копирование без существенного влияния на работу пользователей и приложений, становится недопустимо малым.

5.3 Репликация данных

Современные дисковые массивы обладают средствами создания копий данных внутри самого массива. Данные, созданные этими средствами, носят название Point-In-Time (PIT)-копий, т. е. фиксированных на определенный момент времени. Существует две разновидности средств создания PIT-копий: клонирование и «моментальный снимок» (snapshot). Под клонированием обычно понимают полное копирование данных. Для него требуется столько же дискового пространства, как и для исходных данных, и некоторое время. При использовании такой копии нет нагрузки на дисковые тома, содержащие исходные данные. Иными словами, нет дополнительной нагрузки на дисковую подсистему продуктивного сервера.

Механизм работы «моментальных снимков» иной и может быть реализован как программно на продуктивном сервере, так и аппаратно внутри массива. В момент, когда необходимо начать резервное копирование, программа-агент дает команду приложению завершить все транзакции и сохранить кэш-память на диск. Затем создается виртуальная структура — snapshot, представляющая собой карту расположения блоков данных, которую ОС и другое ПО воспринимает как логический том. Приложение прерывает стандартный режим работы на короткое время, необходимое для сохранения данных. После этого приложение продолжает работать в стандартном режиме и изменять блоки данных, при этом перед изменением старые данные блока с помощью драйвера snapshot копируются в область кэш-памяти snapshot и в карте расположения блоков данных указывается ссылка на новое местоположение блока. Таким образом, карта snapshot всегда указывает на блоки данных, полученные на момент завершения транзакций приложением. Блоки данных, которые не были изменены, хранятся на прежнем месте, а старые данные измененных блоков — в области кэш-памяти snapshot. Программа-агент копирует непротиворечивые данные, полученные на момент завершения транзакций приложением, осуществляя доступ к ним через драйвер snapshot, т. е. используя карту расположения блоков. Создание копий с помощью «моментальных снимков» экономит дисковое пространство, но создает

дополнительную нагрузку на дисковую подсистему продуктивного сервера. Какой из методов создания PIT-копий выбрать, решается на этапе проектирования системы резервного копирования, исходя из бизнес-требований, предъявляемых к системе.

6. Выводы

Итак, подводя итоги, можно сказать, что резервное копирование является очень важным процессом в функционировании серверов и баз данных как больших организаций и бизнесов, так и персональных компьютеров. Существуют разные системы резервного копирования, отличающиеся технологиями создания резервной копии, допустимыми размера копии, функционалом работы с копиями, скоростью восстановления, а также ценой. Каждый пользователь или организация выбирает такую систему, которая наиболее подходит под их нужды и запросы. Как показывает опыт больших компаний, основанный на достаточно долгой дистанции, нельзя пренебрегать резервным копированием, так как с помощью этого инструмента можно очень быстро восстановить, казалось бы, утерянные данные. И это относится не только к большим корпорациям, но и к обычным пользователям, например, студентам. Может произойти сбой в операционной системе, который удалит вашу выпускную работу, и можно потерять все, что было наработано в течении полугода или более. Однако, выполняя регулярное резервное копирование, можно восстановить документ потеряв намного меньше информации. Не стоит пренебрегать резервным копированием. Несколько минут потраченные на создании копии могут сохранить вам месяцы или даже годы работы по восстановлению утерянных данных.

7. Литература

1. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО "Мир и семья-95", 1997. — URL: http://bugtraq.ru/library/books/attack1/index.html

2. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: http://bugtraq.ru/library/books/attack/index.html

3. Запечников С. В. и др. Информационн~пасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.

4. Статья в электронном журнале «Хабр»: «Система резервного копирования» https://habr.com/ru/post/421251/

5.Статья в электронном журнале TADVISER: «Система резервного копирования» https://www.tadviser.ru/index.php/Статья:Система_резервного_копирования