Резервное копирование виртуальных сред

С давних времен человечество старалось сохранить наиболее важные данные в каком-либо виде — начиная с каменных табличек и заканчивая твердотельными энергонезависимыми накопителями. Сегодня, в цифровую эпоху количество информации, необходимой для гарантированного хранения, непрерывно растет. И для её обработки требуются всё более мощные и сложные системы.

В последние годы средства обработки информации (операционные системы, базы данных и приложения) все чаще переносятся в виртуальную среду, что позволяет более эффективно использовать вычислительные ресурсы и увеличивать надёжность систем. Конечно, при текущем уровне отказоустойчивости система продолжает работать при практически любых отказах аппаратных средств, но все же риск повреждения самих данных пока никто не отменял. Для того чтобы обеспечить высокий уровень сохранности данных приходится использовать средства резервного копирования.

На данный момент уже существуют несколько систем виртуализации, хорошо зарекомендовавших себя для использования в промышленных системах. Самая известная и популярная из них принадлежит компании VMware. Ее догоняют, по функциональным возможностям, продукты Microsoft Hyper-V, Citrix XenServer/Desktop, Red Hat KVM. Но мы рассмотрим механизмы резервирования именно для семейства продуктов VMware vSphere.

Упомянутые выше продукты виртуализации серверов относятся к типу логического разделения ресурсов и используют особенности защищённого режима процессора x86. Виртуальная машина является контейнером, внутри которого функционирует независимая копия гостевой операционной системы. Таким образом, на одном физическом сервере (хосте) могут сосуществовать ОС различных типов: Windows, Linux, x86 UNIX, MS-DOS. Фактически виртуальная машина является папкой на файловой системе, резервную копию которой легко создать, скопировав ее на другой носитель.

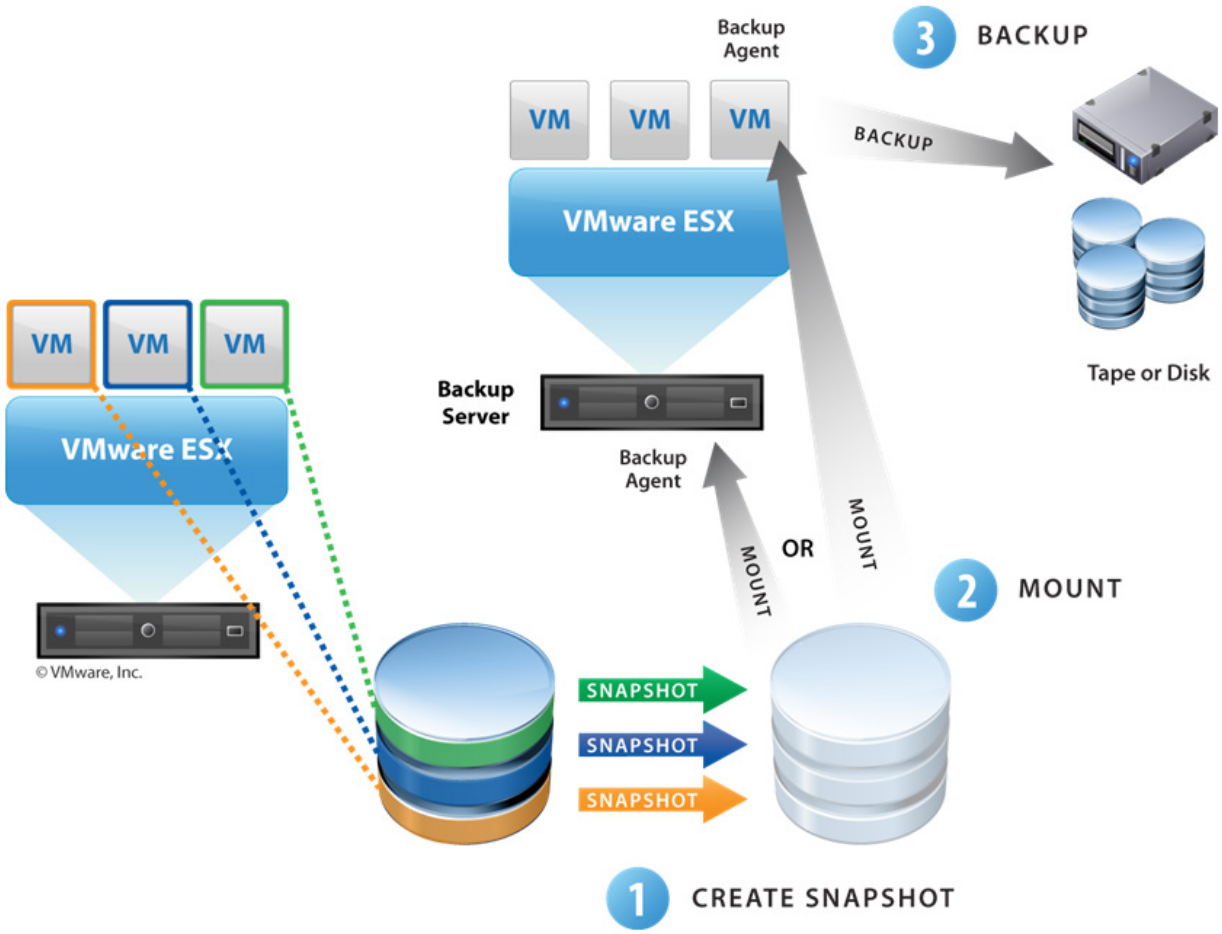
Сложности с резервированием виртуальных машин начинаются в момент резервирования по «горячему», потому что в этом случае нельзя гарантировать консистентную копию данных. При взгляде на виртуальную машину изнутри мы видим, что это как бы физический сервер, и он полностью в нашем распоряжении, поэтому нет никакого ограничения на использование уже имеющихся систем резервного копирования с возможностью создания резервных копий без остановки приложений или операционной системы. Покупаем специализированного агента системы резервного копирования, устанавливаем внутри виртуальной машины, настраиваем и спим спокойно – наши данные сохранены.

С другой стороны, легкость управления виртуальными машинами (мобильность, клонирование, развёртывание из шаблонов, отсутствие перерасхода вычислительных ресурсов и исполнение давней мечты системных администраторов «одно приложение на один сервер») приводит к тому, что количество виртуальных машин начинает расти методом ненаправленного взрыва. И всех их нужно резервировать, т.е. приобретать агент резервного копирования на каждую виртуальную машину, что гарантированно увеличит как финансовые затраты, так и затраты на администрирование.

Поначалу всё так и было. Стоимость резервного копирования росла, но выгоды от виртуализации были несравненно выше. Позже производители систем резервного копирования изменили условия лицензирования, чтобы повысить конкурентные преимущества своих продуктов. На данный момент в большинстве из них необходимо купить агентскую лицензию на хост и использовать ее на любом количестве виртуальных машин внутри этого хоста, не покупать на каждую виртуальную машину. Из этого следует вывод, что с точки зрения экономии средств на лицензиях лучше развернуть систему виртуализации на четырёх хостах с четырьмя ЦПУ, чем на восьми с двумя ЦПУ.

Традиционно программное обеспечение систем резервного копирования пересылает данные через локальную сеть, что требует большой пропускной способности и специально зарегламентированных окон резервного копирования. А это не всегда возможно, особенно для организаций, работающих круглосуточно.

Внедрение технологий виртуализации ведет к консолидации, что создает возможность забирать данные всех виртуальных машин напрямую с системы хранения, на которой они находятся. При таком подходе есть недостаток - виртуальная машина не знает, что её данные кто-то копирует и что нужно приостановить запись на диск или закрыть файлы. Решается эта проблема в VMware vSphere с помощью VMware Tools и VMware Consolidate Backup (VCB). Первое позволяет уведомлять машину о каких-нибудь манипуляциях с ней, второй — интегрировать систему резервного копирования с системой виртуализации: получать прямой доступ к данным , уведомлять о манипуляциях и других операциях, предоставляемых VCB.



Как видно из рисунка, на первом этапе виртуальная машина уведомляется о начале резервного копирования и делается её снимок, чтобы зафиксировать состояние файловых систем. На втором этапе снимки подключаются к системе резервного копирования. На третьем полученные данные сбрасываются на виртуальные или обычные ленточные библиотеки.

Такая простая и понятная схема позволяет снизить связанную с резервным копированием нагрузку на виртуальную машину, а также реализовать резервное копирование без использования сети передачи данных. То есть все данные передаются через SAN (Сеть Хранения Данных), что ведет, в том числе, к уменьшению нагрузки на сеть и сокращению времени резервного копирования.

Следующим этапом эволюционного развития стала передача функций VCB непосредственно в программное обеспечение резервного копирования. После публикации VMware vStorage API ведущие производители систем резервного копирования встроили поддержку прямого доступа к ресурсам системы виртуализации. Данный шаг позволяет отказаться от VCB, увеличив надёжность, убрав дополнительное ПО из цепочки копирования. Тем самым отпадает необходимость и в выделенном сервере под VCB. На текущий момент поддерживается оба механизма.

Никому не нужно резервировать информацию, но всем нужно её восстанавливать — так говорят пропагандисты систем резервного копирования. И с ними действительно трудно не согласиться. Основным неудобством восстановления являлось то, что необходимо было восстанавливать всю машину целиком, для «тяжёлых» машин это могло занимать до нескольких часов, даже если бы понадобилось восстановить всего несколько файлов. На текущий момент во многих системах резервного копирования внедрено гранулярное восстановление данных, которое позволяет восстанавливать удалённые файлы прямо в виртуальную машину без её остановки. Такие механизмы были реализованы, например, в продуктах фирмы Symantec NetBackup и BackupExec.

С момента распространения систем виртуализации появились и нишевые средства резервного копирования, например, продукты компаний Veeam и Vizioncore. Но эти продукты хороши при условии, что все системы, данные которых необходимо резервировать, являются виртуальными машинами. В ситуации, когда существуют приложения, работающие в физической среде (а на сегодняшний день обычно так и бывает), или используется ПО, не сертифицированное для работы внутри виртуальной среды, например, БД Oracle, придётся внедрять дополнительную систему, Поэтому оптимально внедрять сразу универсальную систему резервного копирования, одинаково успешно работающую как в физической, так и в виртуальной среде. Например, Symantec NetBackup полностью сертифицирован для VMware vSphere и Microsoft Hyper-V, может резервировать операционные системы, работающие на x86, Sun SPARC, IBM Power и HP Itanium серверах, а также интегрируется с приложениями и базами данных (Oracle, Lotus, SAP и др.). Полный список сертифицированных систем можно найти на сайтах производителей.

В заключение хочется сказать, что системы резервного копирования для виртуальных сред стали достаточно зрелыми для внедрения в промышленные системы любой сложности. Поэтому ваши данные утеряны не будут.

www.ot.ru

ОТКРЫТЫЕ ТЕХНОЛОГИИ

Россия, 117485, Москва, ул. Обручева, 30/1, строение 2
Тел.: +7 495 787 0888, 787 7027. Факс: +7 495 787 7028
www.ot.ru

01.04.2010