Миграция с VMware на OpenStack с минимальным даунтаймом

В эпоху тотальной автоматизации, когда дело касается корпоративной инфраструктуры, бизнес особенно обеспокоен вопросом ее безопасности. Опытные руководители ИТ-отделов понимают: если вся площадка или какая-то ее часть выйдет из строя, большинство бизнес-процессов остановится. Это сулит серьезные неприятности — по данным агентства Aberdeen, финансовые потери за час простоя инфраструктуры составляют в среднем 164 тысячи долларов.

Спрашивать за убытки и недополученную прибыль в этом случае будут с ИТ-отдела. Осознавая всю степень ответственности, ИТ-директора пытаются добиться от руководства выделения бюджета на приобретение сервиса Disaster Recovery (восстановление после сбоев). Однако часто получают отказ — слишком дорогое удовольствие. Но так ли это на самом деле?

И да, и нет. Дело в том, что подавляющее большинство компаний использует в качестве платформы виртуализации продукты типа VMware vSphere, Microsoft Hyper-V и другие. Разумеется, в случае использования коммерческого ПО, клиент платит за лицензии. И платит, надо сказать, много, — около 7,5 тыс. долларов на один сервер с поддержкой на три года. Зато продуктив работает стабильно — и все довольны.

Как только разговор заходит о приобретении лицензий у того же, например, VMware для резервной площадки, руководители компаний только разводят руками. Потому что стоят они не меньше, чем на основную. А удваивать бюджет готовы не все.

ИТ-отделу остается только ограничиваться резервными копиями. А где их развернуть, если инфраструктура выйдет из строя? Ответа на этот вопрос часто нет.

План восстановления после аварий имеют только 55% компаний (согласно отчету Forrester Research и Disaster Recovery Journal). То есть потребность в DR испытывают многие, но спрос, особенно на российском рынке, сдерживается высокой стоимостью программного обеспечения. Конечно, вопрос в цене каждого часа простоя и в том, как руководство компании оценивает возможность аварии. Дополнительным фактором, тормозящим развитие рынка DR в России, можно назвать дефицит отечественных разработок в этой сфере.

Специалисты по работе с открытым кодом решают вопрос создания бюджетного DR-продукта в комплексе. С одной стороны, они создают инструмент, позволяющий в принципе отказаться от лицензионных выплат. С другой — развивают сервисную модель реализации DR-сценариев, то есть избавляют потенциального заказчика от капитальных расходов на оборудование. Кроме того, DRaaS существенно снижает риски, возникающие в связи с дефицитом компетенций на стороне заказчика. Согласитесь, не каждый ИТ-отдел среднестатистической компании сам сможет построить облако на базе ПО с открытым кодом для размещения полноценной резервной копии. Да и процесс миграции с VMware на OpenStack довольно трудозатратен и неясен. И потом, где развернуть такой “франкенстек”? Покупать еще один, дублирующий комплект оборудования? Такое приобретение может свести на нет всю экономию на лицензиях…

Именно поэтому сервис-провайдеры задумались о том, как удовлетворить потребности корпоративных клиентов, не обременяя их лишними расходами. Так, компания ATLEX заключила партнерское соглашение с российским DR-стартапом Hystax. В рамках партнерства инженеры обеих компаний разработали уникальный сервис восстановления после сбоев на базе OpenStack.

Причем здесь Disaster Recovery, если речь в этом материале должна пойти о миграции с платформы VMware на OpenStack? — спросите вы. И мы ответим: создание резервной площадки и плана восстановления данных — это самый очевидный, пусть и не единственный, сценарий миграции. Судите сами: вы проверили облако провайдера при работах по созданию резервной площадки: развернули копию своей инфраструктуры, провели “учебные пуски” DR-плана, возможно, использовали резервную площадку для нагрузочного тестирования новых приложений… Все это обошлось вам существенно дешевле лицензионных отчислений и платы за поддержку для основной площадки. В этом случае не только у технических специалистов, но даже у бухгалтерии возникнет банальный вопрос: зачем платить больше? Тогда может быть принято решение о переносе основной площадки с VMware на OpenStack. Технически оба сервиса — DR и миграция — организованы идентично. Поговорим об этом подробнее.

Пошаговое руководство. Не все сразу

Сперва мы изучаем инфраструктуру клиента и по итогам создаем план Disaster Recovery. После этого, совместно с заказчиком, корректируем его, учитывая индивидуальные потребности компании. В среднем весь процесс подготовки плана для предприятия, использующего 300 виртуальных машин, занимает около двух с половиной недель. Собственно, такой же план готовится и для миграции. Мы исследуем особенности существующей у клиента архитектуры: топологию сети, настройки, связи и зависимости приложений, чтобы полностью воссоздать ее в том же виде на OpenStack.

Следующий этап — начальный перенос данных в облако (full-репликация) и тестовый запуск резервной площадки. Клиент имеет возможность убедиться в том, что инфраструктура работает исправно, и только после этого мы считаем проект согласованным.

Как мигрировать данные: демо на пальцах

Попробуем описать, что именно происходит в момент миграции данных.

По условию задачи мы имеем платформу виртуализации под управлением VMware vSphere, на которой у нас расположено 22 виртуальные машины. Данные с них мы хотим перенести на резервную площадку в облако OpenStack.

На основную инфраструктуру клиента, а конкретнее — на тот же хост, где располагаются “виртуалки”, которые мы собираемся защищать, — ставим так называемого “агента”. Это виртуальная машина, которая работает на Linux.

Фактически мы даем заказчику ссылку на файл, который он загружает себе на vSphere, после чего агент начинает работать.

Он запускается и исследует все виртуальные машины вокруг себя. Спустя пару минут в интерфейсе Hystax Acura (так называется описываемое решение) о них появляется информация, которую агент обновляет каждые 30 секунд.

Основное управление агентом происходит через административную панель, в которой администратор может просмотреть имена машин, их IP-адреса, дату последней репликации, размер и т.д. Здесь же можно при желании вручную отменить защиту какой-то конкретной машины.

Имя	IP адрес	Размер	Статус
rhel7.2	192.168.15.100	30,0 ГБ	Реплицируется
memcached9	192.168.15.18	16,0 ГБ	Реплицируется
memcached8	192.168.15.17	16,0 ГБ	Реплицируется
memcached7	192.168.15.16	16,0 ГБ	Реплицируется
memcached6	192.168.15.15	16,0 ГБ	Реплицируется
memcached5	192.168.15.14	16,0 ГБ	Реплицируется
memcached4	192.168.15.13	16,0 ГБ	Реплицируется
memcached3	192.168.15.12	16,0 ГБ	Реплицируется
memcached2	192.168.15.11	16,0 ГБ	Реплицируется
memcached11	192.168.15.20	16,0 ГБ	Реплицируется
memcached10	192.168.15.19	16,0 ГБ	Реплицируется

После сбора “агентурных данных” мы запускаем full-репликацию. Время, которое потребуется для того, чтобы перенести все данные в облако, зависит от ширины канала и размера реплицируемых машин. Но в среднем этот процесс занимает около получаса.

Обратите внимание: когда мы впервые поставили агента на инфраструктуру, все девайсы появляются в интерфейсе как незащищенные (unprotected). Мы выбираем, какие машины (все или несколько) мы хотим реплицировать, и запускаем первую полную репликацию. Ее, к слову, проводим минимум раз в месяц из соображений безопасности.

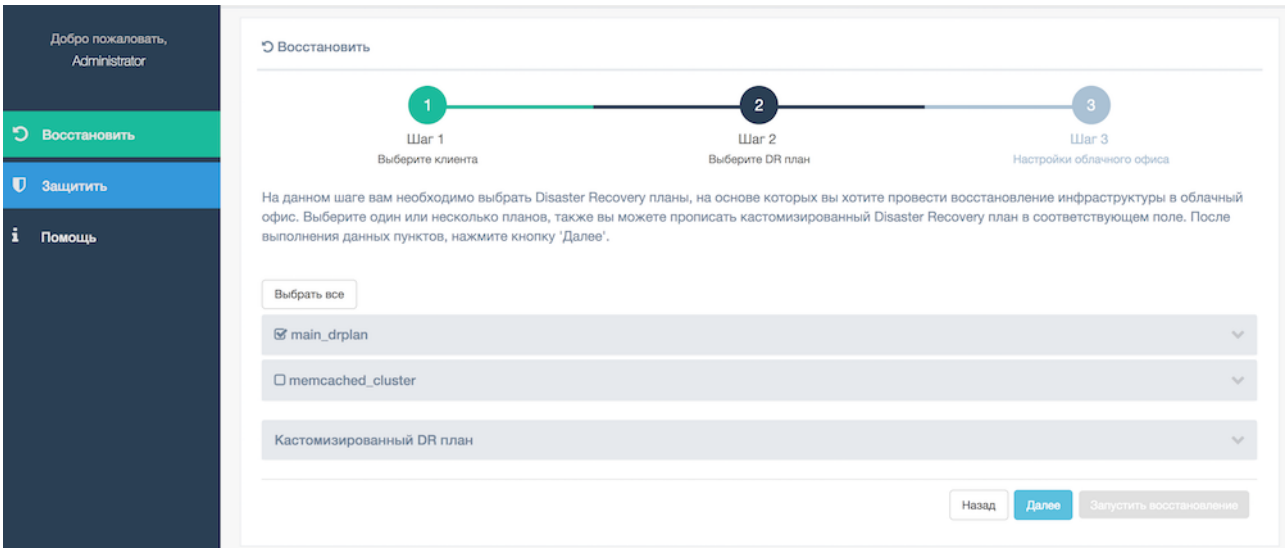
Но мы понимаем, что одной полной репликации данных недостаточно. Ведь данные на основной площадке постоянно изменяются. Поэтому время от времени, по расписанию, которое выбирает заказчик, мы проводим инкрементную репликацию — агенты отслеживают все изменения на инфраструктуре клиента и передают снапшоты в хранилище. Можно выбрать интервальную репликацию или непрерывную — здесь все зависит от поставленной задачи и предпочтений клиента.

Все реплицируемые данные лежат в хранилище. Мы используем метод дедупликации, чтобы сократить объем данных, подлежащих хранению. Если клиент отдал 200 терабайт, то по факту может храниться всего 100. Эффективнее применять этот метод, если реплицируемые машины работают на одной операционной системе или хранят повторяющиеся данные — тогда они будут отосланы и сохранены только один раз. Это, разумеется, скажется и на стоимости хранилища: платить клиент будет за реально занимаемое место.

В случае аварии на основной инфраструктуре клиент просто нажимает на волшебную зеленую кнопку и данные разворачиваются на резервной площадке.

Притча о волшебной кнопке

Если у клиента “падает” инфраструктура, ему действительно нужно нажать на кнопку с надписью “Восстановить”. При этом он может как выбрать восстановление по заранее подготовленному DR-плану (если необходимо восстановить всю инфраструктуру), так и прямо в процессе восстановления создать новый план для нескольких машин (если требуется только их восстановление). Здесь же можно указать дату и время — до какой точки во времени нужно восстановить инфраструктуру.



Система сама “достает” нужные данные из хранилища. Причем выбирает ближайший в прошлом успешный снапшот каждой виртуальной машины. Поэтому за актуальность данных можно не беспокоиться. Кстати, если есть необходимость

восстановить, скажем, информацию месячной давности, эту опцию тоже можно выбрать в настройках.

После того, как виртуальные машины будут восстановлены на резервной площадке, они получат соответствующий статус в интерфейсе. Администратор может запустить “виртуалку” и наоборот — завершить ее работу или вовсе удалить.

Попробовав все прелести резервной площадки на OpenStack и убедившись, что нет никакого смысла переплачивать за лицензии вендоров, заказчик может и скорее всего решит переехать в продакшн на OpenStack. Возможно, он сразу пришел именно за услугой миграции с VMware.

В любом случае, он сам выключает машины на коммерческой платформе (после того, как мы сделали резервные копии), когда новая площадка запущена. При полной миграции клиент получает прямой доступ к своей инфраструктуре.

Заключение

Итак, если перед вами стоит стратегическая задача оптимизировать ИТ-расходы в компании, то одним из путей ее решения может стать полная миграция с коммерческой платформы в облако OpenStack. Сервис-провайдер берет на себя все обязательства по переезду, а вы избавляетесь от необходимости делать лицензионные отчисления и платите только за реально используемые ресурсы.

Если же на данном этапе вас больше интересует надежность вашей инфраструктуры, но вопрос оптимизации расходов тем не менее стоит ребром, то идеальным решением для вас станет сервис восстановления после сбоев (Disaster Recovery). Вы получаете возможность синхронизировать процессы на двух площадках: основной, работающей на коммерческой платформе виртуализации, и резервной — на OpenStack. На случай аварии в дата-центре, внешней вирусной атаки или землетрясения вы будете иметь готовый DR-план. Нажатие одной кнопки — и все ваши данные развернутся на резервной инфраструктуре с минимальным временем простоя, что сэкономит ваши деньги. В свободное от спасения вашего бизнеса время на резервной площадке вы можете, например, тестировать свои новые приложения.

Мы не сомневаемся, что вы по достоинству оцените функциональность нашей облачной платформы, и однажды такого рода репетиции натолкнут вас на мысль, что переплачивать за продукты от вендора вовсе не обязательно.