# Облако ЦОДов, или Сон разума

*Не так давно на одном из важных научно-технических советов я обнаружил в выступлении главного конструктора информационных систем одного из уважаемых ведомств потрясшую меня метафору – он описал облачную инфраструктуру как совокупность «облака ЦОДов, облака „серверов доступа" и подключенных к ним сервисов, таких, как документооборот, безопасность, почта» и других такого же уровня. «Облако ЦОДов» меня потрясло. Я понял, что нужен рассказ, даже не статья, поясняющий основы предметной области, пусть и без конкретики реализаций тех или иных принципов.*

*Ниже я попробую это сделать*

***В. А. Конявский,*** *доктор технических наук, научный руководитель ВНИИПВТИ*

За последние десятилетия мощность компьютеров выросла на многие порядки, человек же, хотя, возможно, и стал умнее, но точно в меньшей степени. Чаще – умнее не стал, хотя человечество в целом значительно продвинулось вперед. Работая на персональных компьютерах, человек, как правило, использует их возможности совсем незначительно, и чем дальше, тем меньше становится относительная доля востребованных среднестатистическим пользователем ресурсов своего ПК. Быстродействие мозга не изменилось, оно остается, как и много лет назад, примерно на уровне 50 операций в секунду. Тактовая частота компьютеров измеряется гигагерцами. Все, что может человек, – это загрузить компьютер на единицы процентов.

Мы платим за 100 % ресурсов компьютера, а используем, например, 2 %. В 50 раз переплачиваем! Жалко.

Конечно, если человек станет платить в 5 раз меньше, то ему это будет выгодно. Если ресурсы компьютера разделить на 20 человек, и каждый начнет платить за 10 % ресурсов, то и владелец компьютера останется в ощутимой выгоде, тем более что на оплату энергетики будет уходить в разы меньше средств. Вот такие рассуждения и явились причиной появления систем виртуализации.

На маленьком компьютере можно поддерживать немного виртуальных машин (ВМ). Очевидно, что чем мощнее компьютер, тем больше ВМ может на нем работать, и тем эффективнее будет виртуализация. Конечно, в том случае, если бóльшая часть ВМ будет использоваться. Мало их создать, нужно, чтобы они были востребованы.

Если компьютер достаточно мощный, и все его ресурсы уже заняты, а ВМ не хватает, тогда нужно покупать еще один компьютер. Станет их много – и тогда потребуется строить специальное инженерное сооружение, эффективно обеспечивающее энергетикой компьютеры, на которых функционируют ВМ. Все вместе это называется ЦОД – центр обработки данных. Пользователь знает, на каком ЦОД размещается его ВМ, но не знает, на каком именно физическом сервере.

Доступ к ВМ для клиента можно организовывать по-разному. Например, если на ВМ установить терминальный сервер, то клиенты могут получать доступ в терминальном режиме. Web-сервер обеспечит web-доступ.

Чтобы получить в свое распоряжение ВМ на ЦОД, нужно понять, какими именно ресурсами эта машина должна располагать, и попросить администратора создать именно такую ВМ. Однажды созданная, ВМ останется именно такой до тех пор, пока не будет изменена или удалена администратором. Другими словами, мы наблюдаем статическое распределение ресурсов. Пользователь знает, где именно находится его ВМ, и что она из себя представляет.

Несколько ЦОД иногда объединяются одним механизмом управления. Теперь ВМ могут размещаться не только на разных физических серверах, но и на разных ЦОД. Но до сих пор пользователь при желании может точно установить, где находится его конкретная виртуальная машина.

Так может продолжаться до тех пор, пока ресурсов группы ЦОД хватает для размещения всех требуемых виртуальных машин. Рано или поздно все ресурсы ЦОД окажутся занятыми, и тогда придется «уплотняться».

Заказывая себе ВМ, мало кто удержится от того, чтобы заказать ее «на вырост». Конечно, за заказанные ресурсы нужно платить, но не так уж и много, и, значит, лучше взять «про запас». В результате, хотя эффектив-

ность использования ресурсов в ЦОД намного выше, чем при использовании ПЭВМ, все-таки оптимальным его не назовешь. Каждый взял себе по 20–30 % запаса ресурсов, значит, свободные ресурсы есть, а использовать их нельзя. Неэкономно получается.

Вот только здесь появляется потребность в том, что отличает «облако» от виртуализации оборудования. Это – динамическое распределение (выделение) ресурсов. «Облако» характеризуется виртуализацией оборудования, виртуализацией ОС, виртуализацией приложений и динамическим распределением ресурсов.

При работе «в облаке» ВМ может размещаться на любой памяти, исполняться на любом сервере любого ЦОД, входящего в состав облачной инфраструктуры. Говорят, что ВМ «мигрируют» между ЦОД. Решение о миграции ВМ принимает «планировщик», исходя из различных соображений, например из логики равномерности загрузки ЦОД, цены ресурсов, просто наличия свободных ресурсов, и др. Не принимается во внимание только (!) уровень конфиденциальности информации, обрабатываемой в ВМ.

Таким образом, облачные технологии начинаются тогда, когда исчерпаны все ресурсы ЦОД, предоставляющих пользователям виртуализированное оборудование на основе использования систем виртуализации. Облачная инфраструктура – это взаимодействующие на основе специализированного «планировщика» ЦОД, средства доступа и клиентские машины. Защищенная облачная инфраструктура – это защищенные серверы, защищенные ЦОД, защищенные ВМ, защищенный доступ (web и/или терминальный), и, наконец, защищенный планировщик, планирующий миграцию ВМ из соображения, в том числе, защищенности информационных ресурсов.

«Облако» есть совокупность перечисленного. Не бывает «облака ЦОДов», не бывает «облака серверов доступа», не бывает «облака сервисов», бывает облачная инфраструктура в целом и облачные сервисы, скрывающие от пользователя всю эту сложную механику и предоставляющие доступ к нужным ему ресурсам.

Теперь важно понять, когда же приходит пора переходить на облачную инфраструктуру?

Сначала нужно сделать ЦОД.

Затем развернуть систему виртуализации оборудования.

Создать виртуальные машины.

Установить на них необходимое ПО.

Разместить на ЦОД информационные ресурсы.

Подключить к ВМ пользователей.

Дождаться, когда пользователи начнут использовать 70–80 % ресурсов.

И только тогда пора задуматься об «облаке».

Здесь мы намеренно опускаем вопросы защиты – не надо создавать защиту «облака», не научившись защищать виртуальные машины.

Если сегодня вы используете ресурсы ЦОД на 0,5 %, и в ближайший год планируете увеличить эту цифру на порядок – не стоит думать об «облаке». Например, если в вашем ЦОД 1000 (тысяча – это немного) физических серверов, и на каждом из них можно поднять 50 (пятьдесят – это немного) виртуальных машин, то 50 000 (пятьдесят тысяч – это много) рабочих мест вполне могут поддерживаться и без облака. Вот если **на этом же ЦОД** вам нужно обеспечить комфортную работу 100 000 сотрудников, то пора подумать о планировщике, и, соответственно, об организации облачного доступа. Если же в вашей корпорации численность одновременно работающего персонала еще не скоро достигнет последней величины, или если у вас уже есть ЦОД, которые в состоянии поддержать достаточное количество ВМ, не надо вам создавать корпоративное «облако». Используйте в полной мере возможности ЦОД.

Если же, несмотря ни на что, вы все же создаете корпоративное «облако», то мотивировать вас может только одно – от публичного «облака» корпоративное отличается защищенностью. В этом смысле построение незащищенного корпоративного «облака» вызовет удивление и у специалистов, и, думаю, у финансовых контролирующих органов.

Вот теперь наступает время поговорить о защите корпоративного «облака».

Таковое можно считать защищенным, если, как минимум:

- обеспечена доверенная среда на компьютерах пользователей;
- защищен доступ пользователей к ВМ (web или терминальный);
- обеспечен контролируемый старт серверов ЦОД и ВМ на серверах;
- защищены ресурсы ВМ;
- обеспечена контролируемая миграция ВМ (то есть используется защищенный планировщик).

Эти меры могут сильно расширяться, но без перечисленных выше говорить о защищенности облачной инфраструктуры нельзя.

Опишем кратко возможные варианты и средства защиты.

1. ***Доверенная среда на компьютерах пользователей*** может создаваться с применением СЗИ НСД (например, это СЗИ НСД семейства «Аккорд» (или аналогичные)) или средства обеспечения доверенного сеанса связи (СОДС) (например, «МАРШ!» или аналогичные);

2. ***Защищенный доступ пользователей к ВМ*** можно обеспечить применением VPN в доверенной среде для web-доступа или системой доверенной загрузки терминальных ОС (например, «Центр-Т», основанной на применении СКЗИ «ШИПКА», «КАМИ-терминал» и др.);

3. ***Контролируемый старт (доверенная загрузка) системы виртуализации*** обеспечивается специализированными СЗИ НСД (для Vmware это, например, «Аккорд-В.» и анало-гичные ему, для MS HV – «Гипер-Аккорд»);

4. ***Защита ВМ*** осуществляется СЗИ НСД, устанавливаемыми в гостевую ОС (например, «Аккорд-VE» или аналогичными ему);

5. ***Системы защиты планировщиков «облака»*** еще находятся в разработке, но очевидно, что их появление – вопрос ближайшего будущего.

Каждый из этих пунктов в дальнейшем будет раскрыт в отдельных статьях под общей серией «Облако ЦОДов». ■