

Преимущества виртуализации ИТ-инфраструктуры средствами компании VMware для предприятий госсектора



Антон Антич,
глава представительства
VMware в России

«Сегодня много говорится о формировании инновационной экономики. Но как можно ее создать, если по оценкам экспертов ее фундамент – ИТ-инфраструктура – находится у нас в стране на уровне конца прошлого века? Пока только наиболее передовые отечественные компании и организации подтверждают, что прогрессивные технологии, к которым относятся и виртуализация, реально работают и приносят ощутимые выгоды. Среди них лидеры нашей экономики – РЖД, МТС, Альфа-Банк, ТНК-ВР. Пора и другим последовать их примеру!»

Организации ищут возможность снижения затрат, более эффективного использования активов, сокращения времени и упрощения внедрения ИТ-решений и управления ими. Виртуализация способна помочь решить все эти проблемы.

Источник: Gartner

Согласно результатам исследований современные организации, в том числе относящиеся к госсектору, могут позволить себе вкладывать в инновации и в создание конкурентных преимуществ менее 30% ИТ-бюджетов, поскольку более 70% они вынуждены расходовать на поддержку эксплуатируемых ИТ-средств. Что же касается доли инвестиций в ИТ-инфраструктуру, то в общем объеме расходов на ИТ они составляют лишь 5%.

Такая структура ИТ-бюджета противоречит требованиям информатизации госсектора, на которую взят курс правительством страны. Виртуализация ИТ-инфраструктуры позволяет резко снизить операционные расходы на ИТ и вкладывать средства, сэкономленные благодаря ее использованию на обслуживании ИТ-инфраструктуры, в развитие информационных технологий.

При тех темпах развития, которые ожидают сегодня от государственных предприятий и организаций, на первый план выдвигается оптимизация расходов. Поэтому важнейшим стимулом для структур госсектора применять виртуализацию является возможность удовлетворять с ее помощью растущие потребности в ИТ-ресурсах не за счет расширения ИТ-инфраструктуры и найма новых специалистов для ее обслуживания, а благодаря экономному использованию имеющихся ИТ-средств и эффективному управлению ими.

Как показывают расчеты и опыт внедрений, благодаря применению виртуализации капитальные затраты на ИТ снижаются на 50–60%, расходы на текущее ИТ-администрирование – на 33%, а расходы на потребление электроэнергии в ЦОДах – на 80%. Подсчитано, что виртуализация в нашей стране одних серверов (без распространения этой технологии на настольные вычислительные системы) позволит за три года только на расходах на электроэнергию сэкономить около 90 млрд руб. Отсюда следует, что 90–95% всех финансовых затрат на обслуживание не виртуализированных серверов в стране в буквальном смысле расходуется на нагревание окружающей среды. Принимая во внимание взятый правительством курс на энергосбережение, виртуализация реально способствует решению государственных задач.

Важным стимулом для применения виртуализации является гибкая поддержка отказоустойчивости серверов. В виртуальных средах ситуация, когда из-за выхода из строя физического сервера прерывается доступ ко всем связанным с ним ИТ-ресурсам, в принципе не может возникнуть, поскольку технологии виртуализации компании VMware разделяют связь между виртуальными серверами и физическим оборудованием, поддерживающими их функционирование. Благодаря этому любой виртуальный сервер может перемещаться с одного физического сервера на другой без перерывов в пользовательских сессиях. Это обеспечивает еще и значительную экономию физических ресурсов, а также позволяет исключить их простой при минимальном вмешательстве человека (или даже исключить его вовсе). Используя виртуализацию, можно автоматически сформировать вычислительные ресурсы с уровнем доступности «пять девяток» за 5 минут при стоимости от 5 центов в час. Без виртуализации на это требуется 6–8 недель при цене за поставку нового физического сервера от 5 тыс. долл. и последующих проблемах с настройкой, обслуживанием, резервированием, восстановлением. . .

Как показывают исследования компании Gartner, экономия средств является главным стимулом применения виртуализации только на первом этапе ее внедрения. Затем на передний план выступает обеспечиваемая ею гибкость использования ИТ-ресурсов. Путь заказчика по дороге виртуализации выглядит как движение от первичной очаговой виртуализации, которая на первом этапе обеспечивает экономическую эффективность, через виртуализацию бизнес-систем и далее к построению гибкой инфраструктуры, которая включает в себя предоставление ИТ как сервиса.

Виртуализация позволяет:

- ◆ создать по-настоящему эффективную ИТ-инфраструктуру;
- ◆ значительно экономить финансовые, энергетические и человеческие ресурсы;
- ◆ обеспечить гибкость и отказоустойчивость ИТ-инфраструктуры, остро необходимые предприятиям госсектора;
- ◆ использовать заложенные в ней практически неограниченные возможности масштабирования ИТ-инфраструктуры.

Защита информации и выполнение требований регуляторов в виртуальной среде

В условиях стремительного роста одновременно исполняемых приложений в сети предприятия резервы технологии «одно приложение – один сервер» практически исчерпаны. Выходом из сложившейся ситуации стала виртуализация – функционирование нескольких виртуальных хостов на одном физическом сервере – и облачные вычисления, где понятие сервера для конкретного заказчика вообще теряет смысл. Но...

Согласно результатам исследований компании Gartner сегодня 40% виртуальных машин (ВМ) устанавливаются без участия специалистов по информационной безопасности (ИБ). По прогнозам аналитиков это приведет к тому, что к концу 2012 года около 60% виртуальных серверов окажутся менее защищенными, чем физические. По этой же причине использование виртуализации затрудняет обеспечение соответствия регулятивным требованиям к защите информации.

В России к этой проблеме в значительной части ЦОДов добавляется необходимость соблюдения требований регуляторов, которые в своих руководящих документах про виртуализацию, увы, ничего не говорят. Особую озабоченность вызывает применение технологий виртуализации при обработке конфиденциальной информации как с точки зрения обеспечения реальной безопасности, так и возможности выполнения требований уполномоченных госорганов. Российское законодательство формирует требования защиты для определенных категорий информации (так называемая информация ограниченного доступа), обрабатываемой в том числе в информационных системах. Какая информация должна защищаться в России по закону? Это конфиденциальная информация, к которой относятся несколько видов тайн («коммерческая тайна», «служебная тайна», «банковская тайна» и т. п.) и персональные данные физических лиц. Также есть законодательные требования по защите информации, составляющей государственную тайну.

Насущными для ИБ-специалистов стали анализ рисков, разработка моделей угроз и нарушителей, связанных с эксплуатацией виртуальной инфраструктуры (ВИ). При этом нужно понимать, что ввиду особенностей виртуальной среды (ВС) для обеспечения ее безопасности в целом средств, применяемых для защиты физической ИТ-инфраструктуры, недостаточно – по причине появления ИБ-угроз, характерных только для ВС.

Специфические ИБ-угрозы для виртуальной среды

Администратор ВИ – новый “суперпользователь”. Наиболее опасным потенциальным нарушителем, располагающим мощными средствами для атак ВС, является администратор ВИ.

Гипервизор – новая цель атак. Гипервизор выступает в ВС в роли суперагента, управляющего одновременно несколькими ВМ, и поэтому является для злоумышленников привлекательным объектом атак, захватив который можно получить суперполномочия сразу над всеми ВМ, управляемыми гипервизором. Компрометация гипервизора создает классическую ситуацию атаки типа «человек посередине», в качестве которого может выступать как внешний нарушитель, так и суперпользователь. При этом гипервизор может обращаться к данным ВМ даже тогда, когда они выключены.

«Виртуализация» трафика. Часть сетевого трафика между ВМ не покидает пределы физического хоста и не попадает в традиционные шлюзовые системы противодействия вторжениям (межсетевые экраны, системы IDS/IPS и т.п.). Поэтому эти средства защиты не могут противостоять как атакам с хостов на ВМ, так и атакам между ВМ.

Смешивание ВМ, обрабатывающих сведения разной степени конфиденциальности.

В силу природы виртуализации без принятия надлежащих мер на одном физическом сервере могут оказаться ВМ, обрабатывающие информацию разной степени конфиденциальности, что недопустимо по соображениям ИБ. Более того, такие технологии, как VMotion, автоматически перемещающие ВМ между хостами, в состоянии сделать это и без участия оператора.



Роман Ермолаев,
коммерческий директор
компании «Код Безопасности»

«Продукты нашей компании хорошо известны на рынке информационной безопасности более 10 лет. В этом году представлено несколько программных продуктов для защиты высокотехнологичных инфраструктур, которые либо не имеют конкурентов, либо на достойном уровне конкурируют с лидерами рынка. Теперь наши предложения – это централизованные комплексные решения сертифицированной защиты от несанкционированного доступа с развитым функционалом сетевого экранирования и сегментации распределенных сетей обработки данных».

Сертифицированная защита среды виртуализации

Компания «Код Безопасности», входящая в группу компаний «Информзащита», предлагает комплексное решение сертифицированной защиты среды виртуализации VMware с помощью программных и аппаратных средств защиты информации собственной разработки.

Security Code vGate for VMware Infrastructure (далее – vGate)

– единственное на российском рынке средство защиты информации от несанкционированного доступа, которое реализует защиту ВС, построенной на платформах VMware vSphere 4 и VMware Infrastructure 3, а также обеспечивает соответствие ВИ требованиям российских и международных регуляторов в части защиты информации.

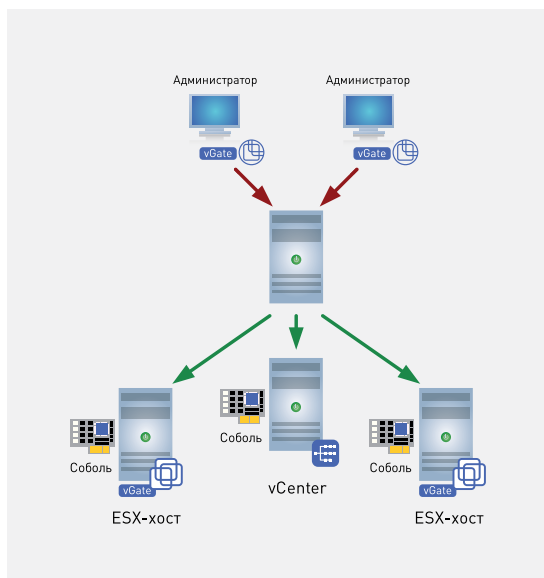
vGate: разделение полномочий и ролевое управление доступом (SoD и RBAC).

Администраторы ВИ разделяются по полномочиям управления сегментами ВИ, обрабатывающими ту или иную группу информации. ИБ-администратор ВИ уполномочен конфигурировать ВС с помощью vGate в соответствии с установленной категоризацией информации и правилами использования информации разных категорий, контролировать соблюдение этих правил, анализировать ИБ-события и соответственно реагировать на нарушения ИБ, не имея при этом доступа к информации.

Модули vGate. Для администраторов ВИ сервер vGate играет роль сетевого шлюза, контролирующего их доступ к хостам по внутреннему протоколу управления VMware и по протоколу SSH. Клиентские модули vGate, устанавливаемые на рабочих местах администраторов ВИ, поддерживают идентификацию и аутентификацию администраторов. vGate также защищает образы VM от скачивания из хранилища на рабочие станции администратора ВИ, оставляя за ним лишь управление их настройками.

vGate: соответствие регулятивным требованиям в области ИБ.

vGate версии 1.0 имеет сертификат ФСТЭК РФ по 4-му уровню контроля на отсутствие НДВ и по 5-му классу защищенности СВТ, что позволяет использовать этот продукт для защиты автоматизированных систем до класса 1Г включительно и информационных систем персональных данных (ИСПДн) до К1 класса включительно. vGate версии 2.0, выпуск которого намечен на июнь, а завершение сертификации на декабрь 2010 года, будет иметь сертификат ФСТЭК РФ по 2-му уровню контроля на отсутствие НДВ и по 3-му классу СВТ, что позволит применять продукт в автоматизированных системах до класса 1Б включительно и обрабатывать государственную тайну до категории “СС” включительно. Кроме того, в vGate 2.0 будут предусмотрены настройки на выполнение российских требований к ИСПДн на соответствие международному стандарту PCI DSS и отраслевому стандарту Банка России СТО БР ИББС.



Таким образом, vGate помогает решить задачи, связанные с аттестацией средств защиты информации указанных выше категорий в ВС, построенной на платформах VMware vSphere и VMware Infrastructure. Делегирование обеспечения ИБ самостоятельному продукту, настоятельно рекомендуемое экспертами ИБ, снимает также проблему сертификации обновлений средств виртуализации.

ПАК «Соболь»: аппаратно-программный модуль доверенной загрузки. Может осуществлять доверенную загрузку ESX 3.5/ESX и компьютеров под ОС Windows (доверенная загрузка vCenter Server).

Следует также обратить внимание на защиту технологических каналов передачи информации – сети передачи данных (Storage Area Network) и передачи данных vMotion/ Fault Tolerance. Хороший вариант – физически изолировать данные каналы передачи информации от остальных сетей.

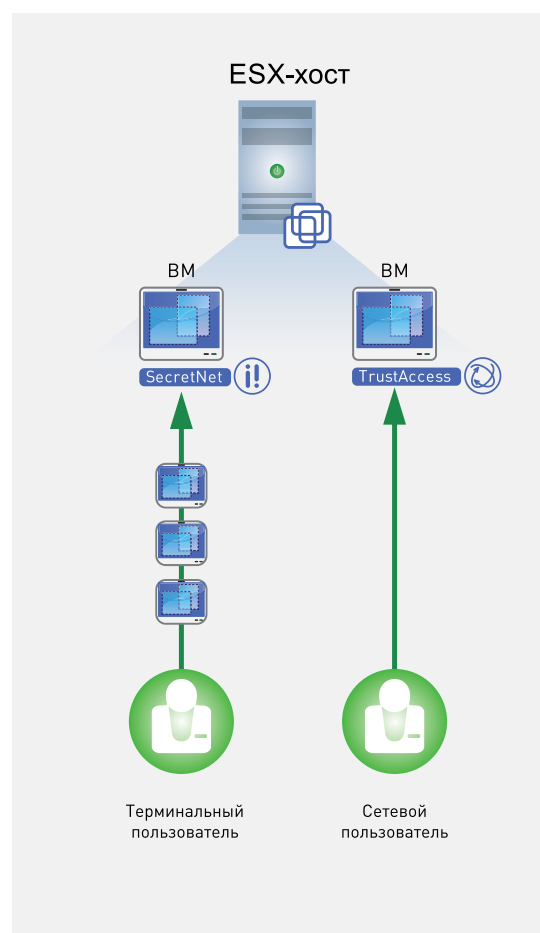
Сертифицированная защита виртуальных машин

Поскольку конфиденциальная информация обрабатывается именно в виртуальных машинах, то они подлежат защите. Картина применения средств защиты очень близка к тому, как защищаются обычные физические компьютеры, но есть несколько особенностей.

Для защиты VM не всегда применимы сертифицированные аппаратные средства защиты ввиду того, что они не были разработаны с учетом эксплуатации в ВС. Большинство программных средств защиты могут применяться для защиты как физических, так и виртуальных машин, но есть особенности, связанные с защитой от несанкционированного доступа.

К физической машине есть 2 типа доступа: сетевой и локальный. Сетевой доступ к VM с точки зрения информационной безопасности аналогичен физическому. Особенность заключается в том, что зачастую сертифицированный межсетевой экран требуется разместить внутри ВС (в виде агента на защищаемой виртуальной машине или в виде отдельной виртуальной машины – Virtual Appliance). Здесь может быть применимо сертифицированное средство защиты «Кода Безопасности» TrustAccess – распределенный межсетевой экран. Агенты TrustAccess размещаются на защищаемых VM.

Что касается локального доступа, то в случае с VM он перерождается в удаленный терминальный доступ. При этом могут использоваться традиционные сертифицированные средства защиты от несанкционированного доступа, если они поддерживают терминальный режим. Таким средством защиты является продукт «Кода Безопасности» Secret Net. Продукт устанавливается на VM и на компьютере пользователя, устанавливающего терминальное соединение. Secret Net защищает терминальные сессии пользователей, если они работают по протоколам RDP или ICA.



Отзыв OCS о функционале защиты vGate и совместной работе с VMware



Руслан Чиняков,
директор департамента СХД
и инфраструктурного ПО OCS

«Весной 2010 года в рамках программы тестирования аппаратного и программного обеспечения, применяемого при построении инфраструктуры ЦОД, в демоцентре компании OCS был установлен новый программный продукт Security Code vGate for VMware Infrastructure отечественного производителя «Код Безопасности». В этом центре партнерам и их заказчикам демонстрируются продукты Brocade, EMC, Riverbed, Symantec и VMware. Оборудование и ПО позволяют построить модель ЦОД практически любой сложности, в том числе с полным резервированием и катастрофоустойчивостью. Кроме демонстраций центр служит для пилот-проектов, проведения тестов на функциональность и производительность, а также для регулярно проводимых тренингов для партнеров и их заказчиков.

ПО vGate служит для обеспечения сертифицированной защиты виртуальной инфраструктуры. Собственные средства VMware способны обеспечивать безопасность на основе механизма ролевого доступа с интегрированной поддержкой Active Directory или стандартной схеме авторизации Windows (при использовании vCenter) или Linux (при использовании изолированных ESX-хостов). Однако, согласно требованиям регулирующих органов, использования встроенных средств защиты недостаточно.

Совместное использование продуктов VMware с программным обеспечением vGate, прошедшим сертификацию ФСТЭК по уровню СВТ 5 и НДВ 4, дает возможность получить преимущества от виртуализации государственным организациям и компаниям, работающим с персональными данными.

Продукт обеспечивает контроль доступа к хостам ESX, виртуальным машинам и vCenter, доверенную загрузку виртуальных машин, аудит событий безопасности.

Программа состоит из нескольких компонентов – Сервера авторизации, Агента аутентификации и Модулей защиты ESX-сервера. Сервер авторизации и Агент аутентификации устанавливаются на Windows-платформу, а Модули защиты – на ESX-серверы. Установка программы не вызывает сложностей у опытного администратора ESX. После установки требуется провести конфигурирование сервера, процесс настройки детально описан в документации.

После настройки продукта получение доступа к управлению серверами ESX и vCenter возможно только после авторизации на Сервере авторизации vGate. Запустить виртуальную машину на хосте ESX с установленными Модулями защиты vGate без авторизации не получится даже в случае доступа с другой машины, расположенной в управляющей подсети VMware.

Таким образом, продукт решает все возложенные на него функции защиты. Даже если злоумышленник попал в ЦОД, то в худшем случае самое серьезное, что он сможет совершить, – это удалить незащищенные файлы виртуальных машин (которые могут быть восстановлены из резервной копии, если специализированными средствами регулярно проводятся резервное копирование и тестирование восстановления). Сами виртуальные машины предлагается защищать традиционными для гостевых ОС средствами типа Secret Net.

Хотя в настоящей версии не поддерживается защита ESXi-серверов, в будущих версиях разработчик обещал исправить эту ситуацию».

Контакты

Технологическое партнерство VMware и «Кода Безопасности», включающее тестирование продуктов на совместимость, обучение специалистов, поддержку партнеров-интеграторов, внедряющих решения виртуализации у заказчиков, является гарантией технологической и организационной надежности совместных предложений для критически важных проектов.



Компания «Код Безопасности» www.securitycode.ru — российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Компания предлагает комплексные решения обеспечения информационной безопасности сертифицированными техническими средствами, которые применяются для защиты конфиденциальной информации, коммерческой и государственной тайны, обеспечивают соответствие систем обработки персональных данных требованиям законодательства. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий. Более 400 авторизованных партнеров «Кода Безопасности» поставляют продукты и поддержку компании в 70 российских регионах.

«Код Безопасности» входит в группу компаний «Информзащита» www.infosec.ru, которая специализируется в области обеспечения безопасности информационных систем и более 10 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.

127018, Россия, Москва, а/я 55

Тел.: +7 (495) 980-2345,

e-mail: info@securitycode.ru,

www.securitycode.ru



Компания VMware – ведущий поставщик решений для виртуализации инфраструктуры бизнеса, открывающих безграничные возможности перед компаниями любых размеров. Использование лучшей из всех ныне существующих платформ виртуализации – VMware vSphere™ – позволяет компаниям любого уровня сократить капитальные и эксплуатационные расходы, обеспечить непрерывность бизнеса, повысить уровень безопасности и защиту данных и содействовать охране окружающей среды. С доходом в 2 миллиарда долл. за 2009 год, числом заказчиков свыше 170 000 и числом партнеров более 25 000, VMware является признанным лидером в области виртуализации – технологии, внедрение которой является одним из приоритетов CIO. Штаб-квартира VMware находится в Силиконовой долине, а офисы компании – по всему миру. Дополнительная информация о VMware доступна на сайте www.vmware.com.

121099, Россия, Москва, Смоленская площадь, 3

Тел.: +7(495) 9701746

Факс: +7(495) 9701748

e-mail: Moscow@vmware.com

www.vmware.ru