Облако ЦОДов, или Сон разума: доверенная загрузка системы виртуализации

С. С. Лындин, *начальник научно-исследовательского отдела*
С. В. Конявская, *кандидат филологических наук, заместитель генерального директора*
ЗАО «ОКБ САПР»
cd@okbsapr.ru

Итак, цикл «Облако ЦОДов, или сон разума»[1] подошел к разделу, посвященному особенностям обеспечения доверенной загрузки именно систем виртуализации, в отличие от каких бы то ни было еще.

Невозможно не обратить внимание на то, что специфическим в вопросах защиты облачных инфраструктур оказывается далеко не все, и даже не большая часть. Однако пренебрегать этой спецификой, конечно, было бы большой ошибкой.

СЗИ НСД, предназначенные для реальных сред, обеспечивают доверенную вычислительную среду за счет ее корректного старта на СВТ: доверенной загрузки ОС, в ходе которой подтверждается целостность компонентов защиты, работающих в ОС, и дальнейшее функционирование ОС под управлением проконтролированного средства защиты. В условиях терминальной сессии ситуация абсолютно аналогична, просто появляются дополнительные СВТ (терминалы), среда на которых контролируется абсолютно так же, с учетом того факта, что функциональность терминальной ОС (если используется специализированная ОС, а не полнофункциональная) может быть строго ограничена по самой своей сути. Никакого принципиально нового объекта контроля не появляется.

В виртуальной же среде старт системы растянут на другое количество этапов, а не просто на разные СВТ: включение физических серверов → загрузка основных ОС (ОС гипервизора/ ОС с управляющими сервисами) → включение управляющих сервисов → отправка сигнала о включении виртуальной машины (ВМ) → обработка сигнала гипервизором → включение ВМ → загрузка ОС.

Компоненты традиционных СЗИ НСД способны проконтролировать только часть этих этапов, и за скобками при этом остается абсолютно принципиальный этап включения ВМ и загрузка ее ОС (с установленным компонентом безопасности, который также некому проконтролировать). Задача специальных СЗИ НСД, предназначенных для виртуальных инфраструктур заключается именно в этом, а все остальные – можно решить комбинированием традиционных продуктов.

Специализированные СЗИ НСД, предназначенные именно для защиты систем виртуализации, в том числе и сертифицированные, на отечественном рынке присутствуют. Значит, есть из чего выбирать, и необходимы критерии для того, чтобы выбор этот был осознанным.

Однако прежде чем выбирать средство защиты виртуальной инфраструктуры, нужно выбрать саму инфраструктуру, то есть – средство виртуализации. От этого выбора зависит настолько многое в том, как будет в дальнейшем организована жизнь всей системы, что делать его следует точно не только сердцем.

В июле 2014 года был опубликован очередной отчет одной из ведущих исследовательских и консалтинговых организаций – компании Gartner – «Магический квадрант 2014 для инфраструктуры виртуализации серверов архитектуры x86». Пятый год подряд первыми, по оценкам Gartner, стали Microsoft и VMware, причем пятый же год подряд VMware – абсолютный лидер.

Впервые Citrix вышел в сектор нишевых игроков, и если для него это – шаг назад, то для Huawei с нишевым решением FusionSphere (ответвление Xen), которое будет продвигаться на развивающихся рынках, таких как Бразилия, Россия, Индия и Китай – это несомненный шаг вперед.

Очевидно, однако, что на сегодняшний день, если делать сравнение не просто ради красоты анализа, а с целью помочь в выборе, целесообразно проанализировать именно

[1] *Предыдущие публикации цикла см. в [1–3].*

продукты лидеров (как по «квадранту», так и по эмпирически наблюдаемым признакам распространенности в реальном мире): Microsoft Hyper-V и VMware vSphere.

Сравнительный анализ платформ виртуализации

Сравнение будет продуктивным, только если учитывать в качестве критериев объективно применимые ко всем сравниваемым объектам и в то же время, объективно значимые для конечной цели выбора факторы. В качестве критериев для выполнения сравнительного анализа систем виртуализации Microsoft Hyper-V и VMware vSphere представляется целесообразным рассматривать следующие:

- масштабируемость;
- интеграция с хранилищами данных;
- сетевое взаимодействие;
- доступность виртуальных машин;
- поддержка гостевых операционных систем и устройств;
- управление памятью и другими ресурсами хостов;
- развертывание и управление.

Результат сопоставления систем виртуализации Windows Server 2012 and vSphere 5.5 представлен в табл. 1. Необходимо отметить, что набор описываемых в рамках выделенных критериев технических характеристик не является исчерпывающим, поскольку перечисление всех возможностей систем виртуализации привело бы к необоснованному увеличению объема результатов анализа.

Следует особо подчеркнуть, что в рамках настоящего исследования исключена из рассмотрения оценка финансовых затрат на приобретение и эксплуатацию системы виртуализации. Данная мера обусловлена тем обстоятельством, что стоимость того или иного решения может существенным образом изменяться в зависимости от большого набора условий, учет которых в общем случае составляет значительные трудности. Так, к числу факторов, определяющих стоимость внедрения Microsoft Hyper-V и VMware vSphere, в числе прочего относятся:

- состав продуктов, которые необходимо использовать в рамках решения применительно к частным условиям функционирования организации (например, для управления Windows Server 2012 Hyper-V необходимо использовать SCVMM, который не является самостоятельным продуктом и использование которого, в свою очередь, требует дополнительной покупки System Center 2012 Suite), при том что распределение функциональности решения по продуктам в Microsoft Hyper-V и VMware vSphere не является однородным, и это делает практически невозможным объективное сопоставление стоимости;
- размер предоставляемых производителем скидок (может варьироваться от 5 до 40 % в зависимости от объемов поставки и заказчика);
- валюта заказа.

Заметим: хотя стоимость решения, безусловно, является значимым фактором, надежность технологии, ее зрелость, возможность интеграции со сторонними компонентами, обширная экосистема не менее важны, и последняя существенно возрастает, если рассмотрению подлежит организация, эксплуатирующая системы с повышенными требованиями к обеспечению отказоустойчивости и надежности функционирования.

Выводы

Для крупных организаций со сложной неоднородной инфраструктурой VMware vSphere предоставляет значительно более широкий набор возможностей, нежели Windows Server 2012 Hyper-V:

- управление расходом ресурсов, затрачиваемых на хранение виртуальных машин;
- распределенные виртуальные коммутаторы;
- обширную экосистему аварийного восстановления;
- поддержку географически распределенных кластеров (metrocluster) и пр.

Отсутствие реализации в системе указанных выше возможностей может оказывать значительное влияние на надежность ее функционирования.

Например, недостаток Hyper-V, связанный с управлением потребления ресурсов хранилища, может вызвать возникновение ситуации, в которой виртуальная машина с низким приоритетом занимает всю полосу пропускания при выполнении операций ввода/вывода, тем самым снижая производительность виртуальных машин, надежное функционирование которых является критичным. Для сравнения, vSphere реализует функцию Storage IO Control. Она задействуется, если время ожидания превышает некоторый заданный порог. Применяя такие средства управления ресурсами, как доли и пределы (shares и limits), можно управлять серверными ресурсами, используемыми виртуальным сервером, таким образом, чтобы виртуальный сервер, который был скомпрометирован, не затронул другие виртуальные серверы на том же самом хосте. Этот механизм можно использовать для предотвращения атаки «Отказ в обслуживании» (Denial of service), при которой атакованный виртуальный сервер потребляет столь значительное количество ресурсов хоста, что другие виртуальные серверы на том же самом хосте не могут выполнять назначенные им функции.

Следует отметить недостаточный уровень зрелости экосистемы Hyper-V, где не реализован надежный механизм обеспечения аварийного восстановления (Disaster Recovery) уровня предприятия, который позволял бы выполнять проверки восстановления после отказа, управлять восстановлением после отказа, создавать отчеты о проведенных проверках для сотен виртуальных машин. vSphere предоставляет, по меньшей мере, три решения уровня предприятия, обеспечивающих аварийное восстановление.

До последнего времени решение Microsoft выглядело более привлекательным за счет известных преимуществ в масштабируемости. Однако с выходом версии vSphere 5.5, в которой были увеличены максимальный объем RAM на хост, максимальное число виртуальных процессоров на хост, максимальное чис-

Таблица 1. ***Сопоставление технических характеристик платформ виртуализации Microsoft и VMware***

Наименование характеристики	Microsoft Windows Server 2012 Hyper-V 3.0	VMware vSphere 5.5	Результат сопоставления
Общие сведения			
Положение на рынке	В числе «лидеров» «магического квадранта» Gartner. Согласно последнему отчету компании Gartner, уступает VMware vSphere в обоих категориях: «Способность реализации» и «Полнота видения»	«Лидер» (позиция № 1 в «магическом квадранте» Gartner)	***Преимущество vSphere 5.5*** (Является значимым, поскольку получено за счет более высокой оценки поставщиков соответствующего сегмента рынка информационных технологий со стороны авторитетной исследовательской и консалтинговой компании)
Возможность централизованного управления	*Реализовано* (System Center 2012 / VMM (SCVMM 2012))	*Реализовано* (совместное использование vCenter Server и Web Client)	***Равнозначные возможности***
Масштабируемость			
Максимальный объем RAM на хост	4 Тб	4 Тб	***Равнозначные возможности***
Максимальное количество логических процессоров на хост	320	320	***Равнозначные возможности***
Количество узлов на кластер	64	32	***Преимущества Hyper-V 3.0*** (Являются значимыми, поскольку неоправданные ограничения на пиковые характеристики, связанные с масштабируемостью системы, в условиях эксплуатации сложной и неоднородной инфраструктуры виртуализации являются нежелательными)
Максимальное количество виртуальных процессоров гостевой ОС	64	32	
Максимальное количество виртуальных машин в кластере	8000	4000	
Максимальный объем vRAM на виртуальную машину	1 Тб	1 Тб	***Равнозначные возможности***
Максимальный размер гостевого виртуального диска	64 Тб (vhd)	62 Тб (vmdk)	***Равнозначные возможности***
Максимальное количество запущенных виртуальных машин на хост	1024	512	***Равнозначные возможности*** (Преимущество Hyper-V 3.0 не является значимым, поскольку возможность запуска 1024 виртуальных машин на одном хосте при современном уровне загрузки ЦОДов представляется избыточной)
Максимальное количество виртуальных процессоров на хост	2048	4096	***Преимущество vSphere 5.5*** (Является значимым, поскольку неоправданные ограничения на пиковые характеристики, связанные с масштабируемостью системы, в условиях эксплуатации сложной и неоднородной инфраструктуры виртуализации являются нежелательными)
«Зрелость» гипервизора	Место, занимаемое гипервизором на жестком диске: - 5 GB с установкой ядра - 10 GB с полной установкой Windows Server	Место, занимаемое гипервизором на жестком диске 155 Мб	***Преимущество vSphere 5.5*** (Является значимым, поскольку обусловливает более высокий уровень безопасности за счет меньшего объема кода, который требуется защищать и поддерживать. Кроме того, небольшой размер гипервизора позволяет использовать экономически выгодные бездисковые сервера с загрузкой гипервизора с SAN)
Хранение данных			
Поддержка хранилищ данных уровня блока	iSCSI и Fibre Channel	iSCSI и Fibre Channel	***Равнозначные возможности***
Поддержка хранилищ данных уровня файла	SMB	NFS	***Равнозначные возможности***
Управление ресурсами хранилищ данных	*Не реализовано*	*Реализовано* (Storage I/O Control)	***Преимущества vSphere 5.5*** (Являются значимыми в тех случаях, когда системой предъявляются требования: динамического распределения вычислительных ресурсов в зависимости от действительных потребностей каждой виртуальной рабочей станции; обеспечения динамической масштабируемости хранилища данных; оперативного контроля за функционированием технических и программных средств. Перечисленные требования предъявляются большинством систем)
Автоматическая балансировка нагрузки виртуальных дисков без простоев	*Не реализовано*	*Реализовано* (Storage DRS). (пулы ресурсов позволяют гибко объединять и распределять ресурсы частного облака)	
Использование хранилищ на основе профилей. Обеспечивает мониторинг пула хранилищ, оптимизацию и автоматизацию процесса инициализации хранилищ	*Реализовано с ограничениями* (отсутствует автоматическое обнаружение характеристик хранилища, подобное VMware VASA)	Реализовано (vSphere Storage APIs for Storage Awareness (VASA)) (поддерживает все аспекты настройки хостов, в том числе и проверки их совместимости с имеющимся профилем)	

Наименование характеристики	Microsoft Windows Server 2012 Hyper-V 3.0	VMware vSphere 5.5	Результат сопоставления
Перемещение запущенных виртуальных машин с одного хоста на другой без использования разделяемого хранилища	*Реализовано* (Shared Nothing Live Migration)	*Реализовано* (vMotion)	***Равнозначные возможности***
Возможности использования дешевых хранилищ для размещения виртуальных машин с высоким уровнем доступности без SAN	*Реализовано* (поддержка SMB 3.0, JBOD)	*Реализовано* (vSphere Storage Appliance без дополнительной платы)	***Равнозначные возможности***
Миграция хранилищ. Возможность перемещать виртуальные диски без простоя	*Реализовано*	*Реализовано* (Storage vMotion)	***Равнозначные возможности***
Передача нагрузки на сторону дискового массива	*Реализовано* (Offloaded Data Transfer (ODX))	*Реализовано* (vStorage API for Array Integration (VAAI), поддерживается многими производителями)	***Равнозначные возможности***
Обнаружение характеристик хранилища	*Реализовано* (SMI-S)	*Реализовано* (VASA)	***Равнозначные возможности***
Поддержка HBA/SCSI-диска в гостевой ОС	*Реализовано* (N_Port ID Virtualization)	*Реализовано* (NPIV для RDM)	***Равнозначные возможности***
Использование виртуальных дисков с «экономным распределением» ресурсов (thin provisioning)	*Реализовано*	*Реализовано*	***Равнозначные возможности***
Резервное копирование только измененных блоков виртуальных дисков, а не виртуального диска полностью	*Реализовано* (инкрементное резервное копирование VHD, предлагаемое в Windows Server 2012. Необходим DPM 2012 SP1)	*Реализовано* (Changed Block Tracking)	***Равнозначные возможности***
Слияние/удаление снапшотов без перезагрузки виртуальной машины	*Реализовано* (Live VHD merge)	Реализовано	***Равнозначные возможности***
Дедупликация файлов виртуальных дисков	*Не реализовано*	*Не реализовано*	***Равнозначные возможности***
Сеть			
Распределенный виртуальный коммутатор (Distributed Virtual Switch). Позволяет реплицировать конфигурацию коммутатора на другие хосты	*Не реализовано* (коммутатор необходимо создавать вручную на каждом хосте)	*Реализовано*	***Преимущество vSphere 5.5*** (Является значимым, если к системе предъявляется требование централизованного администрирования и мониторинга всех подсистем, входящих в состав системы, на системотехническом уровне. Такое требования предъявляется в большинстве систем)
Поддержка производителем возможности агрегации сетевых интерфейсов без использования сторонних драйверов	*Реализовано*	*Реализовано*	***Равнозначные возможности***
Ранжирование (prioritize) сетевых протоколов	*Реализовано*	*Реализовано*	***Равнозначные возможности***
Распределение по зонам между виртуальными машинами, разрешающее или запрещающее сетевой трафик	*Не реализовано*	*Реализовано* (зоны vShield включены в лицензию)	***Преимущество vSphere 5.5*** (Является значимым, если к системе предъявляются требования к разделению потоков информации с целью обеспечения независимого выполнения технологических процессов в пределах разных контуров безопасности информации)
Непосредственный доступ из виртуальной машины к сетевому хранилищу и устройствам ввода/вывода	*Реализовано* (Single Root I/O Virtualization)	*Реализовано* (Single Root I/O Virtualization)	***Равнозначные возможности***
Разграничение сетевого трафика между виртуальными машинами	ACL для портов, закрытые vLAN	Закрытые vLAN, возможности распределенных виртуальных коммутаторов	***Равнозначные возможности***
Подключение к виртуальным коммутаторам сторонних сетевых средств мониторинга	*Реализовано* (API расширяемого виртуального коммутатора)	*Реализовано* (зеркалирование портов (port mirroring), возможности распределенных виртуальных коммутаторов)	***Равнозначные возможности***
Виртуализация сети. Перемещение виртуальных машин в другие подсети без изменения IP-адреса	*Реализовано* (виртуализация сети в SCVMM2012 SP1)	*Реализовано* (VXLAN)	***Равнозначные возможности***

Наименование характеристики	Microsoft Windows Server 2012 Hyper-V 3.0	VMware vSphere 5.5	Результат сопоставления
Протоколы подключения клиентов к виртуальным машинам	RDP, ICA	RDP, ICA, PcoIP	***Преимущество vSphere 5.5*** (Является значимым, поскольку протокол PCoIP менее требователен к полосе пропускания сети, чем RDP и ICA)
Возможность защиты каналов сетевого взаимодействия в соответствии с требованиями российских регуляторов	*Может быть реализована* сторонними наложенными средствами (VPN)	*Может быть реализована* сторонними наложенными средствами (VPN)	***Равнозначные возможности***
Доступность виртуальных машин			
Восстановление виртуальной машины в случае отказа хоста	*Реализовано* (Failover Clustering)	*Реализовано* (функции высокой доступности VMware High Availability)	***Равнозначные возможности***
Миграция запущенных виртуальных машин между хостами	*Реализовано* (Live Migration)	*Реализовано* (vMotion)	***Равнозначные возможности***
Непрерывное (uninterrupted) восстановление виртуальной машины при отказе хоста	*Не реализовано*	*Реализовано* (Fault Tolerance)	***Преимущества vSphere 5.5*** (Являются значимыми, если к системе предъявляются требования по сохранению работоспособности и обеспечению восстановления своих функций при возникновении различных нештатных ситуаций, включая: • сбои в системе электроснабжения аппаратной части; • сбои/отказы в работе отдельных аппаратных средств; • ошибки, связанные с работой системного программного обеспечения. Такие требования предъявляются к большинству систем)
«Горячая» миграция (metro migration). Возможность миграции виртуальной машины на другой хост с двусторонней задержкой, не превышающей 10 мс	*Не реализовано*	*Реализовано*	
Аварийное восстановление собственными средствами	*Реализовано* (Hyper-V replica)	*Реализовано* (vSphere Replication)	***Равнозначные возможности***
Миграция на узлы за пределами кластера	*Реализовано*	*Реализовано*	***Равнозначные возможности***
Поддержка гостевых ОС и устройств			
Поддержка возможности доступа из виртуальной машины к USB-устройствам, подключенным к хосту	*Не реализовано*	*Реализовано*	***Преимущества vSphere 5.5*** (Не являются значимыми в общем случае, но могут быть рассмотрены в качестве таковых в рамках частных условий эксплуатации системы)
Загрузка с USB	*Не реализовано* (загрузка с USB/Flash поддерживается только в бесплатной версии сервера Hyper-V)	*Реализовано*	
Поддержка последовательных портов	*Реализовано* с ограничениями (последовательный порт виртуальной машины может быть связан только с именованными каналами)	*Реализовано* (последовательный порт виртуальной машины может быть связан с физическим портом хоста, выходным файлом, именованными каналами или сетью)	
«Горячее» подключение CPU, жесткого диска и памяти	CPU, жесткий диск	CPU, жесткий диск (SAS, SATA, SSD), память	***Преимущество vSphere 5.5*** (Является значимым с точки зрения расширения возможностей обслуживающего персонала системы в рамках выполнения периодического технического обслуживания и тестирования используемых технических средств, а также восстановления работоспособности технических средств и программного обеспечения системы в сервисном режиме функционирования)
Поддержка гостевых ОС	Windows Server 2003 и последующие версии, Windows XP и последующие версии, CentOS, Red Hat Enterprise Linux, SUSE Linux Enterprise Server (всего 20 поддерживаемых гостевых ОС)	Windows 3.1/95/98/ NT/XP/Vista /7, Windows Server 2003/2008/2012, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS, Debian, Ubuntu, FreeBSD, Solaris, Oracle Linux и др. (всего 96 поддерживаемых гостевых ОС)	***Преимущество vSphere 5.5*** (Значимость очевидна)
Защита виртуальных машин от вредоносных программных средств без необходимости запуска агента в гостевой ОС	*Не реализовано*	*Реализовано* (vShield Endpoint)	***Преимущество vSphere 5.5*** (Является значимым, поскольку позволяет снизить нагрузку на хост и гостевые ОС)

Наименование характеристики	Microsoft Windows Server 2012 Hyper-V 3.0	VMware vSphere 5.5	Результат сопоставления
Возможность мониторинга служб в гостевой ОС, перезагрузки служб в случае необходимости	*Реализовано* (Failover Cluster VM Monitoring)	*Реализовано с ограничениями* (скрипты или сторонние средства)	***Преимущество Hyper-V 3.0*** (Не является значимым, поскольку связано лишь с обеспечением более высокого уровня удобства использования соответствующих возможностей по сравнению с конкурентным решением)
Графические возможности	RemoteFX (WAN, Adaptive Graphics, USB Redirection, Media Remoting, vGPU). RemoteFX интегрирован с RDP. При использовании в системе виртуальных рабочих мест виртуальных терминальных ферм Citrix необходимо специфическое конфигурирование RemoteFX	1) Расширенная поддержка vGPU (поддержка трехмерной графики, выводимой через графические адаптеры NVIDIA и AMD), Soft 3D (рендеринг 3D-картинки без использования адаптера на основе программных техник с использованием памяти сервера), vDGA (выделение графического адаптера отдельной виртуальной машине), vSGA (использование общего графического адаптера несколькими виртуальными машинами); 2) Горячая миграция VMware vMotion (в том числе перенос виртуальных машин между хостами, в которых установлены графические адаптеры разных производителей); 3) Графическое ускорение для гостевых ОС Linux	***Преимущество vSphere 5.5*** (Является значимым, если к подсистеме виртуализации доставки приложений системы предъявляется требование выполнения в независимой программной среде виртуальных рабочих станций программного обеспечения, предъявляющего повышенные требования к графической подсистеме)
Управление памятью			
«Перевыделение» оперативной памяти (RAM overcommit). Возможность выделять для гостевой ОС объем виртуальной памяти больший, чем доступный объем физической памяти	*Реализовано*	*Реализовано*	***Равнозначные возможности***
Оптимизация работы с оперативной памятью Memory Ballooning. Техника гипервизора по работе с оперативной памятью, которая позволяет запустить на хосте виртуальные машины, совокупная выделенная память которых больше суммарной памяти хоста	*Реализовано*	*Реализовано*	***Равнозначные возможности***
«Прозрачное» разделение страниц памяти. Хранение множества идентичных страниц памяти в физической памяти в единственном экземпляре	*Не реализовано*	*Реализовано*	***Преимущества vSphere 5.5*** (Являются значимыми, если к системе предъявляется требование максимально эффективного использования вычислительных ресурсов за счет большей утилизации мощностей процессоров, оперативной памяти серверов и дискового пространства. Такое требование предъявляется к большинству систем)
Сжатие памяти	*Не реализовано*	*Реализовано*	
Управление ресурсами с помощью механизма долей (memory shares)	*Не реализовано*	*Реализовано*	
Управление ресурсами			
Резервирование CPU и памяти	*Реализовано*	*Реализовано*	***Равнозначные возможности***
Динамическая балансировка нагрузки виртуальных машин	*Реализовано* (Dynamic Optimization с помощью SCVMM 2012)	*Реализовано* (DRS с помощью vCenter Server)	***Равнозначные возможности***
Развертывание и управление			
Развертывание гипервизора	*Реализовано* (с помощью SCVMM 2012 SP1)	*Реализовано* (с помощью vSphere AutoDeploy)	***Равнозначные возможности***
Унифицированное и автоматизированное конфигурирование хоста	*Реализовано с ограничениями* (в отличие от решения VMware – профиль хоста не может использоваться для проверки и обновления соответствия хостов после начального развертывания)	*Реализовано* (vSphere Host Profiles)	***Преимущество vSphere 5.5*** (Является значимым, если к системе предъявляется требование централизованного администрирования и мониторинга всех подсистем, входящих в состав системы, на системотехническом уровне)

Наименование характеристики	Microsoft Windows Server 2012 Hyper-V 3.0	VMware vSphere 5.5	Результат сопоставления
Возможность преобразования физических систем в виртуальные машины (P2V)	*Реализовано с ограничениями* (отсутствует поддержка систем на базе Linux)	*Реализовано*	***Преимущество vSphere 5.5*** (Является значимым с точки зрения расширения: • возможностей по администрированию системы; • возможностей обслуживающего персонала системы в рамках выполнения периодического технического обслуживания и тестирования используемых технических средств, а также восстановления работоспособности технических средств и программного обеспечения в сервисном режиме функционирования)
Контролируемое размещение виртуальных машин	*Реализовано* (более 100 правил)	*Реализовано* (правила affinity, anti-affinity, host affinity)	***Равнозначные возможности***
Возможность запуска виртуальных машин на выбранных хостах кластера	*Реализовано*	*Реализовано* (DRS Host Affinity)	***Равнозначные возможности***
Оптимизированное управление электропитанием	*Реализовано* (Power Optimization)	*Реализовано* (Distributed Power Management)	***Равнозначные возможности***
Резервирование средств управления	*Реализовано* (кластеризация SCVMM 2012)	*Реализовано* (дополнительная лицензия vCenter Heartbeat)	***Равнозначные возможности***
Возможность полного управления виртуальной инфраструктурой посредством web-браузера	*Не реализовано*	*Реализовано* (vSphere Web Client)	***Преимущества vSphere 5.5*** (Являются значимыми, если к системе предъявляется требование централизованного администрирования (включая централизованное управление учетными записями персонала системы, централизованную схему использования средств антивирусной защиты) и мониторинга всех подсистем, входящих в состав системы, на системотехническом уровне)
Использование шаблонов виртуальных машин	*Реализовано с ограничениями* (трудоемкий процесс обновления шаблонов: отсутствует возможность быстрого преобразования из шаблона в виртуальную машину, ее обновления и обратного преобразования в шаблон)	*Реализовано* (• Развертывание виртуальных машин из шаблонов с интегрированной тонкой настройкой для гостевых ОС Windows и Linux; • быстрое преобразование из виртуальной машины в шаблон и наоборот; • легкое обновление шаблонов)	
Управление виртуальными рабочими столами (VDI)	*Реализовано* (Microsoft VDI 2012)	*Реализовано* (VMware View)	***Преимущество vSphere 5.5*** (Достигается за счет использования технологии linked clone, позволяющей достичь существенной экономии места в системе хранения данных. Является значимым, если к системе предъявляется требование максимально эффективного использования вычислительных ресурсов за счет большей утилизации мощностей процессоров, оперативной памяти серверов и дискового пространства. Такое требование предъявляется к большинству систем)

ло логических процессоров на хост, максимальный объем диска VMDK и другие пиковые характеристики, преимущество Hyper-V было практически нивелировано.

Кроме того, существенным недостатком Hyper-V являются ограниченные возможности по централизованному управлению (недостаток, отмеченный, в частности, в отчете Gartner). Отдельные задачи могут быть выполнены либо исключительно с использованием SCVMM, либо с использованием Powershell. В свою очередь, VMware предлагает решение проблемы управления, в рамках которого все операции могут быть выполнены с помощью vCenter Server.

Более того, решение VMware (VMware View) по управлению виртуальными рабочими столами (VDI) по ряду показателей превосходит аналогичное решение Microsoft (Microsoft VDI 2012). В частности, реализованная в VMware View технология linked clone позволяет достичь значительной экономии свободного места в системе хранения данных за счет создания реплики «золотого» образа, относительно которой последующие связанные (linked) клоны используют только изменения диска с ОС и пользовательские данные. Благодаря этому система хранения данных освобождается от необходимости хранения многочисленных копий операционной системы (один системный диск – для множества виртуальных машин), упрощаются процедуры внесения изменений в состав и конфигурацию системного ПО (обновление реплики «золотого» образа распространяется на множество виртуальных машин) и, как следствие, повышается уровень масштабируемости и отказоустойчивости системы виртуализации.

Hyper-V поддерживает меньшее число ОС, используемых в качестве гостевых. Помимо этого, Hyper-V имеет ограничения по поддержке «снапшотов» гостевых ОС семейства Linux (например, при использовании инфраструктуры Hyper-V для

снятия «снапшотов» необходимо перед выполнением резервного копирования временно перевести гостевую ОС Linux в состояние ожидания (suspended)).

В части антивирусной защиты виртуальных машин, в отличие от Hyper-V, в vSphere реализована возможность обеспечения защиты виртуальных машин от воздействия вредоносного кода без необходимости запуска агента в гостевой ОС, что позволяет добиться большей производительности и плотности виртуальных машин на хосте по сравнению с решениями, в рамках которых используются антивирусные агенты. Кроме того, отсутствие необходимости запуска агента в гостевой ОС в общем случае способствует упрощению процедуры автоматического обновления сигнатурных баз средств защиты от воздействия вредоносного кода.

Важным аспектом, потенциально способным составить препятствие к использованию в той или иной организации систем виртуализации, является неочевидность возможности организации защиты каналов сетевого взаимодействия, используемых виртуальными рабочими местами пользователей, в соответствии с требованиями российских нормативных документов с применением отечественных криптографических алгоритмов.

Следует отметить, что среди представленных на российском рынке сертифицированных средств защиты каналов представлены не только аппаратно-программные средства, но и программные решения, а также решения, встраиваемые в средства обеспечения доверенного сеанса связи. Следует отметить, что указанные средства – как класса IPSec, так и класса SSL – не имеют известных проблем совместимости с решениями VMware и Hyper-V.

Для создания защищенного канала клиент VPN должен быть встроен в ОС клиентских рабочих мест и запускаться в начале их работы. При этом серверная часть VPN может быть реализована в виде виртуального сервера. Использование в качестве рабочих мест аппаратных терминалов, на которые ОС загружается по сети или с внешнего устройства, не влияет на архитектуру решения. В настоящее время на отечественном рынке представлена обширная номенклатура подобных решений. Так, ряд отечественных производителей (ФГУП КБПМ, ЗАО «ОКБ САПР», ОАО «Инфотекс», ЗАО «С-Терра», компания Stonesoft) обладают опытом встраивания в ОС Linux, загружаемую с таких устройств: VPN Gate (S-Terra CSP), ViPNet Terminal (Инфотекс), ЗАСТАВА (Элвис-Плюс), LirSSL (Лисси), StoneGate (Stonesoft), МагПро OpenVPN-ГОСТ («КриптоКом»), CSP VPN Gate («Сигнал-КОМ»). Аналогичные решения могут быть реализованы для ОС Windows.

Далее ограничимся в своем рассмотрении VMware vSphere как средством виртуализации и сравним представленные сегодня на отечественном рынке средства защиты для инфраструктур, построенных на этой платформе.

Сравнение СЗИ НСД для систем виртуализации на базе VMware

Сертифицированные и наиболее распространенные сегодня СЗИ НСД для систем виртуализации на базе VMware vSphere – это vGate разработки компании «Код безопасности» и ПАК «Аккорд-В.» разработки компании ОКБ САПР.

В основе этих продуктов лежат две разные идеологии защиты виртуальных инфраструктур: «управление ролями» (vGate) и «контролируемая среда» («Аккорд-В.»). В первом случае, подходящем для организации работы в рамках четко заданных ролей внутри компании, акцент делается на управлении потоками. В другом – на доверенный старт проверенной системы, в результате чего загружается доверенная среда, все компоненты которой, включая и средства защиты, функционируют корректно и контролируемо.

В основе vGate лежит управление информационными потоками, позволяющее разграничивать доступ к конфиденциальным ресурсам. Реализуется это следующим образом: все запросы пускаются через специально добавленный в систему сервер авторизации, который фильтрует нежелательные запросы, тем самым выступая в роли межсетевого экрана. Управление доступом «внутри» инфраструктуры производится путем назначения меток элементам инфраструктуры и ее пользователям. Кроме того, производится проверка контрольных сумм файла конфигурации ВМ, файла ее BIOS и главной загрузочной записи.

В основе «Аккорда-В.» лежит «растягивание» контроля старта, реализованного в ПАК СЗИ НСД «Аккорд», на «растянутый» старт инфраструктуры виртуализации: контролируется старт vCenter, старт ESX-сервера, при старте ВМ проводится контроль ее оборудования, BIOS и критичных файлов внутри ВМ, в том числе файлов подсистемы разграничения доступа, далее в каждой ВМ для каждого пользователя создается изолированная программная среда. Контроллеры «Аккорд», используемые в комплексе, могут контролировать файлы ESXi.

Очевидно, что так или иначе оба средства решают задачу выполнения требований российской нормативной базы (более того, они их выполняют, раз являются сертифицированными СЗИ НСД), поэтому несмотря на все принципиальные различия между ними, сравнить их все-таки можно.

Такое сравнение представлено в табл. 2.

Выводы

Необходимо отметить некоторые особенности продуктов, продиктованные их архитектурой, и выглядящие странно, если рассматривать их без ее учета. Так, многие функции vGate дублируют штатную функциональность vSphere. Такое дублирование в случае с vGate – необходимая мера, поскольку для создания доверенной среды, в которой эти функции выполнялись бы vSphere, у vGate нет собственных инструментов, это ПО, а не ПАК (ПАК «Соболь» и ПО SecretNet не являются частью комплекса и устанавливаются (либо не устанавливаются) эксплуатирующей организацией по собственному усмотрению).

Таблица 2. ***Сопоставление технических характеристик продуктов, предназначенных для защиты виртуальных инфраструктур: «Аккорд-В.» и vGate***

№	Наименование характеристики	«Аккорд-В.»	vGate R2 версии 2.6	Результат сопоставления
1.	***Общие сведения***			
1.1	Классы сертификации ФСТЭК	• Действующий сертификат: ТУ, защита АС до 1Г, СВТ-5, НДВ-4, ИСПДн УЗ 1; • действующий сертификат: защита АС на 1Б, СВТ-3, НДВ-2	• Действующий сертификат для версии vGate R2: ТУ, защита АС до 1Г, СВТ 5, НДВ-4, ИСПДн УЗ-1; • действующий сертификат для версии vGate-S R2 vGate-S: ТУ, защита АС до 1Б, НДВ-2	
2.	***Функциональные возможности***			
2.1	Поддерживаемые версии VMware vSphere	4, 4.1, 5, 5.1, 5.5	4.1, 5, 5.1, 5.5	***Равнозначные возможности***
2.2	Самодостаточность средств защиты инфраструктур виртуализации	*Реализовано*	*Не реализовано* (средства доверенной загрузки физического оборудования «Соболь» и ПО разграничения доступа Secret Net для ВМ не входят в состав продукта)	***Преимущество «Аккорд-В.»*** («Аккорд-В.» – завершенный комплекс, достаточный для защиты всех элементов инфраструктуры виртуализации, в том числе и VDI)
2.3	Разделение прав по администрированию виртуальной инфраструктуры и администрирование информационной безопасности	*Реализовано* (• обеспечение аппаратной идентификации и аутентификации при получении доступа к механизмам администрирования; • дискреционное и/или мандатное разграничение доступа администраторов и процессов ко всем ресурсам; • создание изолированной программной среды для каждого администратора; • наличие доступа к инструментам управления системой защиты только у администраторов ИБ и обеспечение их недоступности для администраторов виртуальной инфраструктуры)	*Реализовано* (• разделение прав на управление виртуальной инфраструктурой и на управление безопасностью; • аутентификация администраторов виртуальной инфраструктуры и администраторов информационной безопасности; • полномочное управление доступом к конфиденциальным ресурсам)	***Равнозначные возможности***
2.4	Настройка политик безопасности	*Реализовано* (• мандатный и дискреционный механизм для администраторов виртуальной инфраструктуры, администраторов ИБ и пользователей ВМ; • создание изолированной программной среды)	*Реализовано* (• готовые профили (шаблоны) защиты в соответствии с международными и региональными стандартами; • полномочное управление доступом к конфиденциальным ресурсам)	***Равнозначные возможности***
2.5	Защищенный сетевой доступ к серверам виртуализации	*Реализовано* (• защита терминального доступа со стороны администраторов средствами комплекса; • фильтрация трафика с помощью имеющегося межсетевого экрана)	*Реализовано* (• фильтрация трафика с помощью имеющегося межсетевого экрана; • использование сервера авторизации в качестве шлюза (требует изменения топологии сети); • разрешение сетевого доступа к серверам виртуализации только с доверенных автоматизированных рабочих мест администраторов (по IP-адресу))	***Равнозначные возможности*** (• Проверка IP-адреса, выполняемая vGate, не является надежным механизмом защиты, вследствие чего не может рассматриваться как преимущество; • логика функционирования «Аккорд-В.» не допускает возможности выполнения административного воздействия откуда-либо, кроме защищенного сервера управления)
2.6	Контроль подключаемых устройств ВМ	*Реализовано* (возможность ведения «белого» и «черного» списков устройств, возможность создания изолированной программной среды для каждого пользователя каждой ВМ, контроль целостности файлов внутри ВМ, оборудования ВМ и пр.)	*Реализовано* («белый» список разрешенных к подключению устройств для виртуальной машины, контроль целостности файлов внутри ВМ, оборудования ВМ)	***Равнозначные возможности***
2.7	Взаимодействие с vCenter через web-клиент	*Реализовано*	*Не реализовано*	***Преимущество «Аккорд-В.»*** (• Часть функционала vSphere доступна только через web-клиент; • «Аккорд-В.» сохраняет все функциональные возможности виртуальной инфраструктуры, обеспечивая необходимый уровень защиты; • vGate обеспечивает необходимый уровень защиты за счет исключения отдельных функциональных возможностей виртуальной инфраструктуры)

№	Наименование характеристики	«Аккорд-В.»	vGate R2 версии 2.6	Результат сопоставления
2.8	Поддержка VDI-решений	*Реализовано*	*Реализовано с ограничениями* (• поддерживает только в случае применения без ПО разграничения доступа Secret Net (см. пункт 2.2); • Secret Net не поддерживает работу с XenDesktop)	***Преимущество «Аккорд-В.»*** (более широкая номенклатура поддерживаемых систем без снижения защищенности)
2.9	Интеграция с SIEM-системами	*Не реализовано*	*Реализовано*	***Преимущество vGate*** (более широкая номенклатура поддерживаемых систем)
2.10	Контроль целостности	*Реализовано* (• контроль целостности физического оборудования, гипервизора, виртуальных машин, файлов внутри виртуальных машин и серверов управления виртуальной инфраструктурой; • децентрализованное хранение контрольных сумм ВМ; • использование при расчете контрольных сумм алгоритма ГОСТ; • вычисление контрольных сумм гостевых ОС «извне» ВМ)	*Реализовано с ограничениями* (• контроль целостности исполняемых модулей vGate сервера авторизации, агента аутентификации, vCenter; • контроль целостности файлов ВМ и файлов гостевых систем ВМ; • централизованное хранение контрольных сумм ВМ; • использование при расчете контрольных сумм алгоритма adler32; • вычисление контрольных сумм гостевых ОС «изнутри» ВМ)	***Преимущество «Аккорд-В.»*** (• vGate не позволяет контролировать целостность файлов ESXi; • централизованное хранение vGate контрольных сумм оставляет возможность проведения атак на контролируемые объекты, связанных с нарушением доступности сервера; • известны атаки на используемый vGate алгоритм расчета контрольных сумм; • в vGate для вычисления контрольных сумм гостевых ОС требуются трудоемкие операции, связанные с выполнением настроек и запуском утилиты внутри гостевой ОС)
2.11	Доверенная загрузка	*Реализовано* (доверенная загрузка всех элементов инфраструктуры виртуализации с помощью компонентов, входящих в состав комплекса)	*Не реализовано* (обеспечение доверенной загрузки возможно только при использовании дополнительных средств защиты и расценивается как опциональный механизм, оставленный на усмотрение эксплуатирующей организации)	***Преимущество «Аккорд-В.»*** (• vGate не содержит компонентов, обеспечивающих доверенную загрузку элементов инфраструктуры виртуализации; • в документации vGate декларируется, что «доверенную программную среду ESXi-сервера» обеспечивает «список разрешенных программ, хранящийся на ESXi-сервере»; • при использовании «Аккорд-В.» доверенная загрузка обеспечивается аппаратными компонентами комплекса, дополнительных средств для выполнения этого требования не требуется)
2.12	Централизованное управление (конфигурирование, развертывание, мониторинг)	*Реализовано*	*Реализовано*	***Равнозначные возможности***
2.13	Регистрация системных событий в журнале регистрации, включая детальное журналирование всех попыток запуска серверов	*Реализовано*	*Реализовано*	***Равнозначные возможности***

vGate не предусматривает взаимодействия со средствами защиты на клиентских рабочих местах. Взаимодействие не предполагается даже на уровне получения сведений о том, с защищенного или нет рабочего места начинается взаимодействие с виртуальной инфраструктурой. Поскольку необходимость получения этих сведений становится со временем все более осознаваемой, в том числе и на стадии проектирования систем, разработчиком предложена мера – установка на клиент агента, который авторизуется на сервере. Защитный эффект этой меры не очевиден, поскольку наличие агента, строго говоря, ничего не говорит о качестве среды на клиенте. В то же время взаимодействие с незащищенными клиентскими рабочими местами для ЦОДа способно свести на нет весь эффект от применения средств защиты. Этот фактор необходимо учитывать при планировании защиты системы, принимая во внимание, в частности, материал предыдущей статьи цикла [3].

В программно-аппаратном комплексе «Аккорд-В.» необходимость в дублировании штатных функций vSphere отсутствует, а механизмы, делающие возможным анализ защищенности клиентского рабочего места и предоставление пользователю разного набора прав в зависимости от того, из доверенной ли среды он подключился к ЦОДу, – предусмотрены. ■

ЛИТЕРАТУРА

1. Конявский В. А. Облако ЦОДов, или Сон разума // Защита информации. Инсайд. 2013, № 5, с. 36–37.

2. Чепанова Е. Г., Лыдин С. С. Облако ЦОДов, или Сон разума. Сравнительный анализ решений для обеспечения доверенной загрузки ОС, представленных на рынке // Защита информации. Инсайд. 2014, № 3, с. 56–68.

3. Счастный Д. Ю., Конявская С. В. Облако ЦОДов, или Сон разума: о том, почему необходимо мыть руки перед едой, даже если они «чистые» // Защита информации. Инсайд. 2014, № 5, с. 57–61.