Инфраструктура виртуальных десктопов для клиентских приложений

Статья – представление нового класса решений для разворачивания клиентских приложений на основе их виртуализации, активно продвигающихся на рынке с середины 2007 г. Данная технология реализуется на серверах стандартной архитектуры (x86) и ориентирована на пользовательские ПК.

Введение

Инфраструктура виртуальных пользовательских ПК (Virtual Desktop Infrastructure – VDI), или VDI-решения появились на рынке сравнительно недавно – в 2006 г., а активно стали продвигаться на рынке лишь в прошлом году. VDI-решения это новый подход разделения серверных ресурсов для реализации удаленного доступа к пользовательским ПК.

В отличие от терминальных систем, где каждый десктоп с набором приложений был жестко "привязан" к своему выделенному разделу на сервере, в VDI-решениях каждое десктопное приложение выполняется на отдельной виртуальной машине, работающей на стандартном сервере в датацентре. За счет этого удается достичь значительно большей гибкости в использовании, управляемости и изолированности ресурсов/приложений/пользователей друг от друга.

Общая архитектура построения VDI-решений является дальнейшим развитием терминальных клиентских систем или т.н. тонких клиентов (с максимально "обрезанной" функциональностью, которые, в основном, служили только для визуализации результата работы приложения и транслировании его на удаленный терминал пользователя, а основная нагрузка по его выполнению производилась на сервере), которые появились на рынке еще с 90-х годах и продвигались такими компаниями, как: Citrix, Microsoft, Sun Microsystems и др. Необходимо заметить, что степень разделения ресурсов между сервером и терминальной станцией в каждом из таких решений была своя. Так, например, Sun Ray 1 представлял собой только монитор со встроенными средствами аутентификации пользователей (не имеет IP-адреса и идентифицируется только сервером), в других решениях для терминальной станции использовался ПК (табл. 1). В качестве сервера использовался, в зависимости от задач, или RISC UNIX сервер, или высокопроизводительный x86 сервер. Выбор того или иного решения также в значительной степени определялся лицензионной политикой. Среди основных преимуществ при переходе от клиентских ПК на терминальные системы можно отметить следующие:

- *значительно более высокий уровень доступности/надежности приложений и безопасности данных;*
- *более высокая эффективность администрирования;*
- *снижение нагрузки на локальную сеть;*
- *в ряде случаев снижение ROI и повышение производительности.*

В настоящее время различают 4 типа виртуализации, связанной с реализацией решений для клиентских приложений:

- *<u>серверная</u> – множество приложений и операционных систем выполняются на виртуальных машинах, работающих на высокопроизводительных серверах;*
- *<u>виртуализация на базе одного десктопа</u> (развивается как производителями ЦПУ, например технология Intel vPro, так и производителями ПО, например, продукт VMware Workstation) – множество приложений или операционных систем выполняются на одном локальном компьютере;*
- *<u>виртуализация приложений</u> – позволяет запускать приложения в виде единого исполняемого файла без копирования и развертывания установочных файлов в операционной системе. Таким образом, сохраняется целостность операционной системы: локальная файловая система, файл реестра, политики безопасности и т.п. Это в свою очередь повышает надежность, безопасность и решает проблемы совместимости приложений практически со всеми версиями Windows, начиная с 95. Кроме того, решается проблема конфликта приложений, запускаемых на одном компьютере. К примерам реализации данной технологии можно отнести продукцию компании Thinstall, которая недавно была приобретена компанией VMware;*
- *<u>инфраструктура виртуальных пользовательских ПК</u> – десктопные операционные системы и приложения выполняются на виртуальных машинах, работающих на серверах в датацентре.*

Табл. 1. Сравнение функциональных особенностей реализации трех решений терминальных станций *(конец 90-х)*

Система Sun Ray 1	X-терминалы	MS Windows-based Terminals
ОС исполняется на сервере. Не требуются локальные ресурсы, администрирование.	ОС исполняется на настольной системе. Локальные ресурсы и администрирование.	Требуется Microsoft Windows®CE или встроенный DOS.
Формирование изображения происходит на сервере. На терминал передается готовое изображение.	Изображение формируется в соответствии с потоком команд, посылаемых приложением на X-терминал по протоколу X Windows.	Требуются локальная память, шрифты, драйверы.
Sun Ray 1 – не сетевой узел. Производительность зависит от ресурсов сервера.	Каждая настольная система – сетевой узел. Производительность зависит от локальных ресурсов (процессор, память) и качества сервиса в сети.	Производительность зависит от локальной конфигурации.
Низкая стоимость без ущерба функциональным возможностям (например, мультимедийным).	Ограниченная функциональность во имя сокращения стоимости.	Локальные ресурсы накладывают ограничения на производительность.

Как уже было сказано, последняя технология была представлена на рынке с 2007 г., в основном, тремя компаниями: VMware (после выхода VDI-решения), Citrix (после приобретения Xen) и Sun Microsystems (после интеграции продуктов Tarantella). Данные VDI-решения позволяют использовать для терминальных систем вместо разделяемых реальных UNIX/x86 серверов виртуальные ПК на базе стандартных (x86), что значительно расширяет возможности применения таких реализаций на базе терминальных станций и дает возможность интегрировать в одном решении все преимущества серверной вир-

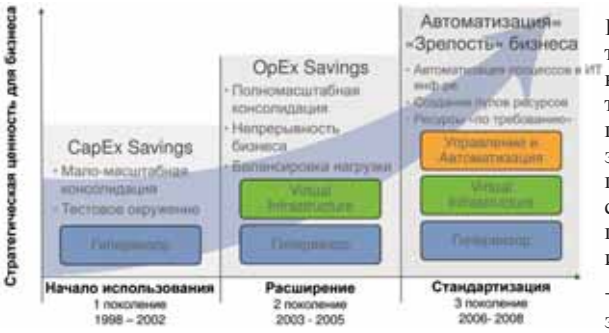

Рис. 1. Эволюция виртуализированных ЦОД на базе решений VMware.

туализации и виртуализации на базе одного десктопа.

VMware определяет виртуализацию приложений как способность развернуть прикладное программное обеспечение без модификации клиентского компьютера и без каких-либо изменений локальной операционной системы, файловой системы и/или системного реестра.

В настоящее время концепция VDI поддержана всеми основными разработчиками ПО и аппаратных компонентов и активно продвигается на рынке.

Тенденции рынка

Несмотря на развивающийся процесс консолидации, число поддерживаемых бизнес-приложений постоянно растет, а сам процесс сопровождения становится все более сложным и более трудоемким, поскольку многие приложения должны работать одновременно и бесшовно связываться друг с другом. Как результат, возрастают простои и число конфликтов между приложениями. По данным Forrester Research, западные компании в среднем тратят более чем $500 в год на поддержку десктопов и управление клиентскими приложениями.

Поэтому уже с 2003 г. на рынке стал разрабатываться инструментарий для упрощения управления клиентской инфраструктурой (ПК, ноутбуки). Среди таких первых решений – OpForce, Radia, Relicor, Altiris, SoftGrid (Microsoft), Ardence (Citrix) и др. Активное развитие (рис. 1) с конца 90-х годов решений по виртуализации серверов стандартной архитектуры привело в 2007 г. к появлению на рынке разработок, которые объединили простоту управления клиентской инфраструктурой и все преимущества терминальных систем.

Если оценивать в целом результат такой эволюции, то переход на более простые автоматизированные средства поддержания клиентских приложений позволяет увеличить число обслуживаемых клиентских компьютеров, приходящихся на одного администратора, с 20–25 до сотен, а виртуальных средах – до тысяч.

Рассмотрим основные особенности и преимущества решения VDI на основе продуктов компании VMware – одной из самых популярных платформ в России и мире.

Основные функциональные особенности VMware VDI-решений

VMware VDI – комплексное решение для создания виртуальных настольных ПК на базе сервера, предоставляющее улучшенный контроль и управление, а также среду настольных ПК, привычную конечным пользователям. Виртуализация парка корпоративных ПК создает множество преимуществ для IT-департамента и конечных пользователей:

– существенное упрощение задач поддержания стандартной корпоративной конфигурации для всего парка ПК: установка приложений, обновлений, диагностика и обслуживание, а также снижение затрат на эксплуатацию и энергозатраты корпоративных ПК;

– централизованное развертывание образов ПК, в связи с чем отпадает необходимость в содержании штата IT-специалистов во всех офисах, филиалах и т.д.;

– возможность использования конечными пользователями любого ПК (обычный ПК, корпоративный ПК, домашний компьютер, компьютер в интернет-кафе и т.д.) или “тонкий” клиент, подключенный к ЦОД) для получения доступа к стандартному корпоративному рабочему месту;

– интеграция виртуальных ПК с инфраструктурой ЦОД, что добавляет такие функции, как резервное копирование, балансировка нагрузки, переход на резервный ресурс, восстановление после сбоев и др.

Помимо названных, есть еще ряд полезных особенностей, ставших доступными в составе решения VDI от VMware.

Повышенная защита данных

В случае внешнего развертывания клиентских приложений обеспечение безопасности доступа/данных может стать большой “головной болью” для многих компаний. Ряд современных коннекторов уже имеют встроенные средства для защиты входа в систему и шифрования трафика. В этом случае встроенные средства шифрования позволяют избежать накладных расходов по управлению доступом к интранет-сети через VPN-клиента. В других случаях VPN третьих фирм будет необходим.

Сетевая транспортная защита (Network Transport Security) для большинства компаний – простой и достаточный способ шифрования трафика с помощью промышленно стандартного SSL-шифрования. Для компаний, имеющих повышенные требования к защите данных, можно использовать стандартное IPSEC-кодирование в Windows, позволяющее шифровать каждый этап/шаг трафика. При этом следует помнить о накладных расходах на CPU для каждой виртуальной машины и каждого ESX-сервера.

Для доступа может использоваться двухфакторная аутентикация на основе RSA SecurID®.

Концепция VDI, или терминальных сервисов усиливает защиту данных по сравнению с удаленными ПК за счет того, что в VDI-решениях можно управлять местом хранения данных, т.е. определять какие данные хранить локально (включая подключаемые USB-диски), а какие – в датацентре, избегая, таким образом, возможной “утечки чувствительных данных”.

Storage-опции VDI-решений

Централизованное хранение данных в VDI-решениях дает возможность использовать такие опции в составе VI3, как VMotion, HA, DRS и DPM в целях улучшения эффективности и снижения затрат. Десктопные приложения обычно не имеют высоконагруженного ввода/вывода в сравнении с серверными приложениями, поэтому не требуют высокопроизводительной инфраструктуры СХД. VDI-решения могут строиться на технологиях типа iSCSI и NFS с использованием большого числа более дешевых SATA-дисков для поддержания datastores серверов ESX, что существенно позволяет снизить общую стоимость инфраструктуры СХД. Учитывая, что каждый десктоп обычно нуждается при-

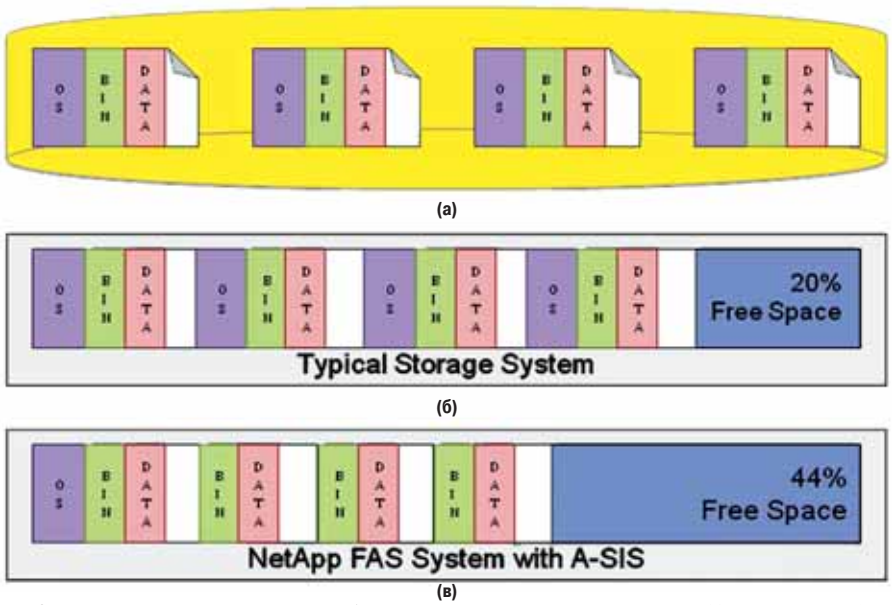

Рис. 2. Распределение емкости хранения без/с использования технологии дедупликации: (а) – VMFS-том с 4 VM (каждый с ОС; местом, занимаемым приложением; данными и свободным пространством); (б) – распределение пространства, занимаемого стандартной системой хранения, использующей VMFS; (в) – пример VMFS-дедупликации VMFS файловой системы, которая на 30% увеличивает емкость хранения.

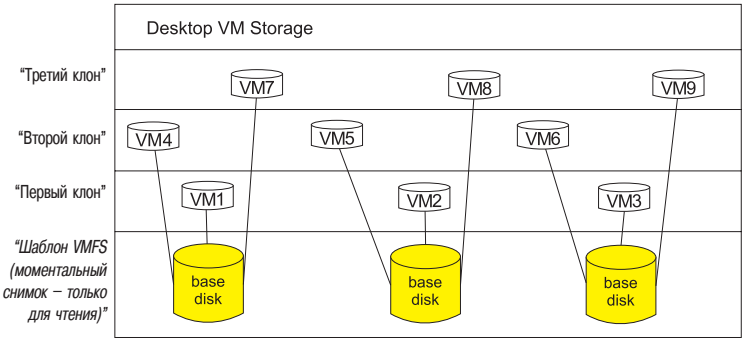

Рис. 3. Пример клонирования VM.

близительно в 8 Гбайт дискового пространства в датацентре, при интенсивном масштабировании инфраструктура хранения может быстро стать узким местом. Поэтому ряд других особенностей/технологий, доступных в VDI-решениях, позволяют уменьшить остроту этой проблемы. Они включают: тонкий провижининг (thin provisioning), технологии дедубликации и Volume- или LUN-клонирование.

Тонкий провижининг. В случае следования лучшим практикам необходимо оставлять приблизительно 20% пространства файловой системы свободным для неожиданного роста данных. Т.о., если все VM виртуальные диски используют 80% своей емкости, и все VMFS-тома также используют 80% своего объема, то общая утилизация системы будет составлять 64% в лучшем случае (не включая различные дополнительные издержки и затраты на организацию RAID).

Тонкий провижининг позволяет распределять неиспользуемую область памяти в глобальном storage-пуле, таким образом увеличивая доступную емкость хранения.

Дедупликация данных *(Data De-duplication)*. Учитывая то, что в VDI-средах развертываются зеркала образов VM, большой объем информации в VM избыточен. Устраняя все избыточные данные через технологии дедупликации первичных файловых систем, можно экономить до 50% и более емкости хранения, требуемой для поддержания виртуальных десктопов, что значительно уменьшает TCO и увеличивает ROI решения. На рис. 2 показано распределение емкости хранения без использования технологии дедупликации (б) и с ее поддержкой (в).

Transparent Page Sharing (TPS) – технология, развивающая предыдущую и позволяющая экономить использование оперативной памяти сервера за счет дедупликации одинаковых блоков оперативной памяти множества VM (рис. 4). Например, в случае VDI-решения на сервере выполняется множество однотипных VM (одна и та же ОС, патчи и приложение), использование технологии TPS позволяет оставлять в ОП только один уникальный блок для всех VM и, соответственно, запускать больше VM на одном сервере, что также положительным образом влияет на стоимость решения.

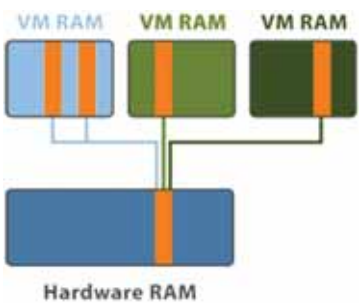

Рис. 4. Transparent Page Sharing – технология позвляющая экономить использование оперативной памяти сервера за счет дедупликации одинаковых блоков памяти множества ВМ.

Известны случаи, когда получаемая при этом экономия ОП может быть многократной. Так, в одной реализации 178 однотипных VM (каждая по 512 Мбайт), с TPS физически расходовали 19,07 Гбайт ОП. Без TPS для них, соответственно, потребовалось бы 512 Мбайт x 178 = 91 Гбайт (экономия – 4,77 раза).

Клонирование тома или LUN. Многие дисковые массивы обеспечивают возможность клонировать LUN или том, позволяя делать моментальные снимки существующей файловой системы и одновременно поддерживая их "читабельность" для кластера ESX. Особенность этой функции в том, что клонируются только измененные блоки данных относительно оригинального тома, за счет чего "клон" занимает существенно меньше места в сравнении с "оригиналом". При этом полностью имитируется, что клон представляет собой полный том. Эта опция активно используется в составе продуктов VMware Workstation/Lab Manager и Stage Manager и позволяет очень быстро назначать большое число виртуальных машин (группа из 10 и более VM может быть выделена в течение от нескольких секунд до нескольких минут) без дополнительного распределения больших объемов хранения.

Так, например, если требуется развернуть 9 VM на базе одной с размером файловой системы 10 Гбайт, то может потребоваться 32,7 Гбайт (вместо 90 Гбайт при недоступности опции клонирования томов в составе системы хранения). При этом с целью распараллеливания процессов доступа к данным клонируются 3 полных базовых диска "только для чтения" (рис. 3) и 9 клонов для VM (32,7 Гбайт = (10 Гбайт x 3 base disks) + (300 Мбайт x 9 differencing disks)).

При этом следует учитывать ограничения использования опции Volume/LUN Cloning в том, что каждый ESX сервер может поддерживать только до 256 LUN. Поэтому может возникнуть потребность сгруппировать ESX серверы в кластеры, основываясь на представлении/организации ресурсов хранения, а также определить оптимальное число VM, хостируемых на отдельном "шаблоне" VMFS (например, при 5 VM на "шаблоне" используемых VM может быть 1280 = 5x256). Однако один "шаблон" может включать 10, 50, 100 и более VM в зависимости от потребности.

Расширенная функциональность продукта VMware ThinApp

В январе 2008 г. VMware завершила приобретение компании Thinstall, которая была пионером в концепции безагентских/безинфраструктурных технологий и внедрения такого инструментария, как Active Directory и PC Configuration Management Tools (используются в составе пакетов: MS SMS, BMC Configuration Management, LANDesk, Matrix42, Altiris и др.). В результате интеграции технологий/решений Thinstall в портфолио VMware уже в ближайшей перспективе (сейчас доступна бета-версия 2, а продукт называется VMware ThinApp, *прим. ред.*) в составе VMware VDI-решений будет доступен ряд уникальных функциональных возможностей:

- ***прямой стриминг клиентских приложений*** – возможность вообще не устанавливать ни клиентов, ни драйверов на клиентском ПК (не конфигурировать ПО в виртуальные машины), поскольку виртуализированное приложение можно непосредственно "стримить", т.е. запускать прямо из сетевого хранилища/общедоступного ресурса (LAN, WAN или Internet) без какой бы то ни было установки и записей в реестр пользовательского виртуального ПК. При этом можно запустить большое количество приложений в течение секунд;
- ***выполнение приложений полностью в непривилегированном режиме*** *(user mode)* – полностью отсутствует какое-либо влияние на операционную систему, что уменьшает риски защиты, вызванные агентами или компонентами, которые нуждаются в привилегиях администратора;
- ***возможность одновременного выполнения множества копий приложения на одном ПК*** – это означает, что можно "упаковать" приложение "А", используя более раннюю версию ThinApp (например, 3.100), и развернуть его на 500 пользовательских десктопах. Позже их можно апгрейдить, например, до версии 3.500, чтобы использовать новые особенности. Одновременно можно развернуть новое приложение "В", используя версию VMware ThinApp 3.500, без какого-либо влияния на ранее развернутое приложение "А". Это может быть критичным, например, тогда, когда множество подразделений компании хотят использовать технологию независимо друг от друга и без необходимости синхронизации версий приложений;
- ***мгновенное развертывание приложений с переносных устройств хранения*** – виртуальное приложение, созданное с помощью VMware ThinApp, может быть легко "записано" на любой переносной носитель типа флэш-диска или CD-ROM и далее в считанные секунду запущено с него. При таком развертывании регистр приложения и изменения файловой системы, предназначенные для хостового компьютера записываются на переносном устройстве. Поскольку виртуализованное приложение не имеет никаких драйверов устройств и выполняется в гостевых учетных записях, то такие переносные приложения могут использоваться на киосках PC, даже если они заблокированы и не разрешают никакой инсталляции;

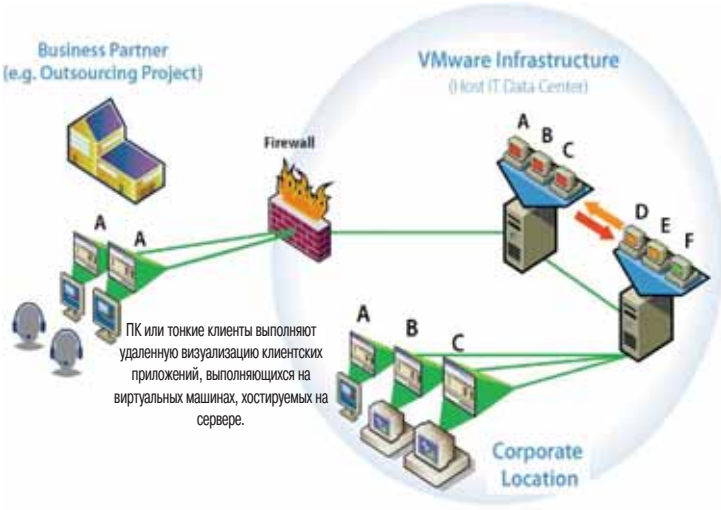

Рис. 5. Два типа имплементации VDI-решений: внутренняя и внешняя.

– ***отсутствие возможности внесения каких-либо изменений (включая данные) в физическую систему*** – все изменения, предназначенные для хостовой файловой системы PC и системного реестра, переадресовываются к пользовательскому хранилищу (private-per-user sandbox). Это хранилище может быть расположено или в сети, чтобы сохранять все пользовательские настройки при его переходе от одного ПК к другому, или на локальном USB-накопителе.

Приложения в среде VMware ThinApp предъявляют минимальные требования к клиентской/хостируемой платформе:

– виртуализированная ОС, которая "внедряется" в состав каждого приложения, занимает 400 Кбайт дискового пространства и менее 2 Мбайт RAM;

– виртуализированные приложения выполняют прямые команды ЦПУ без какой-либо эмуляции или трансляции, что позволяет работать большинству приложений в реальном времени без каких-либо задержек.

Поскольку при загрузке приложений выполняется прямая блокуровневая декомпрессия, то дополнительного места на диске для распаковки приложения не нужно. Когда пакеты приложений развернуты на жесткие диски ПК для автономного использования, дисковые требования также значительно уменьшены, т.к. сами данные приложений остаются сжатыми всегда. Это в целом снижает требования на ресурсы хранения на локальном ПК более чем на 40%.

VMware ThinApp позволяет создавать переносимые приложения, которые могут быть развернуты на разных ОС (Windows NT, XP, Vista, 2000) в различных окружениях (SMS, LANDesk, Citrix, BMC и др.).

Табл. 2. Сравнение особенностей реализации клиентских инфраструктур приложений на трех типах архитектур.

Capabilities	Fully Configured PCs	Shared Application Solutions	Virtual Desktop Infrastructure Solution
Solution	Удаленные ПК выполняют приложения локально.	ПК/тонкие клиенты выполняют удаленную визуализацию клиентских приложений, работающих на выделенном сервере.	ПК/тонкие клиенты выполняют удаленную визуализацию клиентских приложений, выполняющихся на виртуальных машинах, хостируемых на сервере.
Security			
Сохраняемые данные размещаются в высоконадежном корпоративном центре данных		•	•
Удаленная инфраструктура имеет централизованное управление, включая пользовательские права доступа		•	•
Management			
Для управления приложениями и операционными системами используются стандартные десктопные средства управления	•		•
Легкость добавления, модификации, изменения или бэкапирования настольных приложений без вмешательства пользователя		•	•
Быстрая миграция десктопного окружения для смены аппаратной платформы "по щелчку мыши"			•
Изоляция пользователей друг от друга в случае системного сбоя	•		•
Implementation			
Выполнение приложений на десктопе	•		
Выполнение приложений на сервере		•	•
Выполнение приложений без модификаций	•		•
Создание привычного пользовательского интерфейса	•		•
Поддержка любых десктопных платформ		•	•

Особенности развертывания VDI-решений

В общем случае существует 2 типа внедрения решений VDI: внутри корпоративной инфраструктуры и за ее пределами (рис. 5). Вследствие того, что в последнее время все больше компаний становятся децентрализованными с необходимостью доступа к корпоративным данным/приложениям в дороге, командировке, на отдыхе и т.д., особую остроту приобретает проблема управления удаленными клиентскими инфраструктурами. Это связано с проблемами поддержания требуемого уровня безопасного доступа и сервиса приложений, эксплуатацией большого числа разного типа клиентских устройств и ПО управления (часто третьих фирм) и др.

В этой связи использование решений VDI для оффсайтных инфраструктур во многих случаях может принципиально решить многие вышеперечисленные проблемы и существенно снизить эксплуатационные издержки поддержания подобных инфраструктур. В табл. 2 приведено сравнение особенностей трех типов реализации удаленных клиентских инфраструктур.

Законченные решения VDI требуют интеграции с множеством продуктов третьих фирм. Для решения этих задач в 2006 г. был создан VMware Virtual Desktop Infrastructure Alliance. В него вошли 33 члена, среди которых "аппаратные" вендоры, такие как: Sun, HP, IBM, Wyse и ClearCube, а также производители средств управления, безопасности и удаленного доступа, такие как: Altiris, Citrix, Check Point, LANDesk, Novell и Platform Computing и др.

Тестирование показало *(VDI Server Sizing and Scaling, 2006 г.)*, что, например, один сервер класса HP ProLiant DL385 G1 (CPU: два 2-ядерных AMD Opteron 2.2GHz; RAM – 16GB; два Ultra 320 SCSI drives – 2 x 146GB disks, 15K rpm) может поддерживать в среднем до 26 десктопов/пользователей, классифицируемых как "знающие" пользователи и выполняющих задачи маркетинга, управления проектом, продажи, настольных издательских систем, финансового анализа, анализа данных (data mining), исполнительного и контрольного управления и др. Соответственно, для менее интенсивной нагрузки (офисная работа) число десктопов/пользователей на таком же сервере может доходить до 42.

Заключение

Виртуализация десктопной инфраструктуры, значительно упрощающая развертывание и поддержание клиентских приложений, по мнению многих аналитиков, – один из самых "горячих" трендов рынка с объемом более $1 млрд. Эта технология активно поддержана всеми основными игроками, которая уже в ближайшей перспективе будет иметь большое развитие как с точки зрения использования на мировом и региональном рынках, так и появления инноваций для этих решений.