Спрос и предложение на рынке виртуализации

Денис КВАСНОВ,
ведущий инженер департамента инфраструктуры информационных систем компании «АМТ-ГРУП»

Современные среды виртуализации подразделяются на два вида: классическая и контейнерная.
Классическая виртуализация устроена так, что в виртуальной среде выполняются целые виртуальные машины, каждая со своим виртуальным оборудованием, в которых выполняются приложения под управлением разных гостевых операционных систем типа Windows, Linux и т. д.
Контейнерная виртуализация устроена иначе: виртуальная среда запускается прямо из ядра хостовой операционной системы. Вместо нескольких гостевых операционных систем используется одна операционная система хоста виртуализации. В данном случае изоляцию ОС и приложений поддерживает сам контейнер. Одной из популярных платформ контейнеризации является Docker, а для автоматического управления контейнеризованными приложениями есть популярная платформа Kubernetes.
Этот вид виртуализации очень востребован у разработчиков, поскольку она хорошо подходит для создания и развертывания приложений в нескольких средах без многократного переписывания программного кода.

Рассмотрим особенности серверной виртуализации, удовлетворяющей потребности большинства промышленных заказчиков.

Серверная виртуализация повышает эффективность использования вычислительных ресурсов до 80–90%. Например, вместо десяти физических серверов, выполняющих каждый свое приложение, возможно запустить все эти приложения в виртуальной среде и обойтись двумя-тремя серверами виртуализации. Также обеспечивается отказоустойчивость.

Типичная схема отказоустойчивой платформы выглядит следующим образом: серверы виртуализации объединены в кластер под управлением менеджера управления. Менеджер управления знает, какие бизнес-приложения выполняет каждый из серверов. При отказе любого из серверов менеджер перезапускает бизнес-приложения на других работоспособных серверах кластера. Таким образом обеспечивается непрерывность функционирования бизнес-приложений на предприятии заказчика.

Ландшафт отечественного сегмента

Отечественный рынок виртуализации складывался нетипичным образом. Основным драйвером развития были требования регуляторов по использованию отечественного ПО в государственных, окологосударственных и силовых структурах. Для выполнения этих узких задач разрабатывалось специализированное ПО.

В 2022 г. рынок отечественной виртуализации получил приток огромного количества заказчиков из всех отраслей отечественной промышленности. Вместо узкоспециализированных задач появился запрос рынка на замещение полной функциональности систем виртуализации зарубежных производителей.

В настоящее время к основным тенденциям развития сегмента относятся разработка репликации на уровне гипервизора, виртуализация сетей L2–L4, аварийное переключение с основного ЦОД на резервный РЦОД (аналог SRM), репликация на уровне СХД, конвертация v2v, автоматизация процесса обновления инфраструктуры, управление конфигурациями хостов.

Следует отметить актуальность гиперконвергенции. В силу малой доступности на отечественном рынке СХД эта функциональность очень востребована, что также является важным вектором развития.

Популярные решения

Рассмотрим наиболее популярные решения на

отечественном рынке виртуализации. В качестве примеров обратимся к продуктам и решениям отечественных вендоров, которые мы тестировали в нашей лаборатории и используем в своих проектах.

zVirt (разработчик OrionSoft)

Защищенная платформа виртуализации zVirt построена на базе open source продуктов. На базе высокопроизводительного гипервизора KVM (Kernel-based Virtual Machine), системы управления oVirt и библиотеки управления виртуализацией LibVirt. zVirt обеспечивает управление серверами виртуализации, виртуальными машинами, хранилищами, кластерами и другими объектами среды виртуализации из единой консоли с русскоязычным интерфейсом. Успешно применяется для импортозамещения VMware и Microsoft Hyper-V.

В графический интерфейс СУВ zVirt встроена функциональность резервного копирования, возможна работа с системой мониторинга Zabbix, видеокартами в режиме vGPU (GRID). Предусмотрены возможность миграции ВМ между кластерами, мониторинг состояния системы и т. д.

В настоящее время в платформу добавлена репликация и катастрофоустойчивость (Disaster Recovery), что позволяет в случае аварии на основном центре обработки данных полностью или частично восстановить данные на резервной площадке.

В системе обеспечивается конвертация многочисленных виртуальных машин с VMware на zVirt с минимальным временем простоя. Система zVirt работает с большим количеством поколений процессоров, включая поколения ЦП 2010-х годов. Обеспечивается высокая доступность приложений, отказоустойчивая работа виртуальных машин (High Availability), причем миграция ВМ и данных между серверами и хранилищами происходит без прерывания работы. Система имеет возможность интеграции со службами каталога и ролевую модель для назначения прав доступа к средствам управления. В системе реализована балансировка нагрузки ВМ между хостами. В качестве гостевых поддерживаются операционные системы Linux и Microsoft Windows.

Платформа имеет сертификат ФСТЭК, включена в Единый реестр российского ПО.

«Альт Виртуализация» (разработчик «Базальт СПО»)

Система представляет собой сборку Linux, реализующую виртуализацию и контейнеризацию для корпоративной инфраструктуры. На ее основе можно создавать все типы виртуализации: ОС, ПО, инфраструктуры, систем хранения данных, сети. Есть интеграция с системами корпоративной аутентификации (LDAP, MS AD и др.).

Возможна установка гостевых операционных систем любых версий семейства Linux, Microsoft Windows. Предусмотрены четыре сценария установки: базовая виртуализация, классическая виртуализация с изолированными виртуальными машинами, облачная виртуализация и контейнеризация.

Система основана на гипервизоре KVM, утилитах запуска ВМ Qemu и библиотеке LibVirt. Управление виртуальными машинами осуществляется через графический интерфейс приложения virt-manager либо через консоль командной строки virsh.

Платформа включена в Единый реестр российского ПО.

Rosa Virtualization (разработчик «НТЦ ИТ РОСА»)

Среда виртуализации с интегрированной системой управления ROSA Virtualization позволяет развернуть виртуальный центр обработки данных (ВЦОД) корпоративного уровня в кратчайшие сроки.

С помощью русскоязычного графического интерфейса системы управления средой виртуализации (СУСВ), входящей в состав ROSA Virtualization, осуществляется централизованное управление объектами виртуальной среды (гипервизорами, хранилищами, кластерами, дата-центрами, виртуальными машинами и пр.).

Платформа основана на использовании открытого гипервизора KVM, библиотеки Libvirt и VDSM в качестве основных компонентов. Конфигурация, состояние, отчеты и другая вспомогательная информация хранятся в базе данных PostgreSQL.

Система интегрируется с другими приложениями через интерфейсы на основе RestAPI, Python SDK и Java SDK. Система виртуализации может быть интегрирована с доменами Active Directory и FreeIPA.

В качестве гостевых операционных систем поддерживаются дистрибутивы Linux и Microsoft Windows. Доступ к интерфейсам виртуальных машин может быть осуществлен через VNC или SPICE. В случае использования SPICE обеспечивается работа со звуком и USB-устройствами.

Платформа имеет сертификат ФСТЭК, включена в Единый реестр российского ПО.

Следует отметить актуальность гиперконвергенции. В силу малой доступности на отечественном рынке СХД эта функциональность очень востребована, что также является важным вектором развития.

«РЕД Виртуализация» (разработчик «РЕД СОФТ»)

Основу программного продукта «РЕД Виртуализация» составляет система управления виртуализацией с открытым исходным кодом (oVirt). Система управления виртуализацией серверов и рабочих станций построена на базе гипервизора KVM, библиотеки управления виртуализацией LibVirt, OpenSource-проектов Gluster, PatternFly, Ansible и собственных разработок компании «РЕД Софт».

«РЕД Виртуализация» позволяет управлять виртуальными машинами через веб-интерфейс, для администрирования используется библиотека libvirt.

В состав «РЕД Виртуализации» входит реализация веб-интерфейса и служб, необходимых для управления виртуальными машинами. «РЕД Виртуализация» представляет собой образ ОС на основе «РЕД ОС», в состав которого включены необходимые пакеты и репозиторий для установки и функционирования системы виртуализации.

«РЕД Виртуализация» позволяет создавать масштабируемую кластерную систему виртуализации с распределенной системой контроля ресурсов оборудования и полномочий пользователей.

Функции управления виртуальными машинами предусматривают выбор приоритета высокой доступности, живую миграцию, мгновенные снимки в реальном времени, клонирование виртуальных машин из моментальных снимков, создание шаблонов виртуальных машин, использование cloud-init для автоматической настройки во время подготовки и развертывания виртуальных машин. Поддерживаемые гостевые операционные системы включают GNU/Linux, Microsoft Windows и FreeBSD. Реализована интеграция с доменами MS Active Directory, Samba DC, FreeIPA.

Платформа включена в Единый реестр российского ПО.

«СВ Брест» (разработчик ГК «Астра»)

ПК «СВ Брест» построен на базе сертифицированной ОС Astra Linux SE. Программный комплекс предоставляет современный набор инструментов с собственным графическим интерфейсом для управления объектами виртуальной инфраструктуры любого масштаба и сложности. «СВ Брест» предназначен для управления:

- виртуальными машинами и виртуальными рабочими местами (VDI);
- физическими хостами, кластерами и центрами обработки данных (ЦОД);
- сетями, хранилищами и т. д.
- Созданные виртуальные машины могут работать как на Linux, так и на Windows.

Система построена на базе гипервизора KVM, библиотеки управления виртуализацией LibVirt, QEMU и сертифицированных СЗИ. С их помощью на основе архитектуры x86-64 можно эмулировать аппаратное обеспечение и виртуализировать процессоры, создавать защищенную среду виртуализации для серверов и рабочих мест, а также предоставлять удаленный доступ к ним с помощью VDI.

Управление системой с помощью веб-интерфейса дает возможность легко контролировать и администрировать все компоненты виртуальной инфраструктуры.

Продукт поставляется с двумя версиями лицензий: «Стандарт» позволяет использовать в качестве гостевой системы на ВМ только ОС Linux, а «Корпоратив» разрешает применение Windows.

Платформа включена в Единый реестр российского ПО.

HOSTVM (разработчик HOSTVM)

HOSTVM – платформа виртуализации корпоративного уровня на основе гипервизора KVM для виртуализации серверов, рабочих столов, приложений и организации терминального доступа. Ее основу составляют гипервизор HOSTVM и сервер управления HOSTVM Manager.

Для хранения данных может использоваться как гиперконвергентное хранение на локальных дисках (SDS), так и классическая блочная система хранения данных (СХД). В роли резервного копирования может выступать компонент HOSTVM Backup, который обеспечивает базовые потребности в сфере резервного копирования.

Платформа снабжена инструментами миграции для легкого и быстрого импорта виртуальных машин с любой платформы виртуализации: VMware ESXi (через API vCenter), XEN (через API Xen Center), KVM (через API libVirt), Hyper-V, а также файловыми шаблонами виртуальных машин в формате OVA.

Гибкая платформа для виртуальных рабочих мест (HOSTVM VDI) позволяет создавать пулы виртуальных машин для автоматического развертывания ресурсов по мере подключения пользователей. Доступ к графической консоли обеспечивается по протоколам SPICE, VNC, RDP, X2Go, NX, HTML5, PCoIP, Loudplay.

Наличие у продукта сертификата ФСТЭК является определяющим преимуществом для систем виртуализации на предприятиях, являющихся субъектами КИИ.

HOSTVM VDI предусматривает использование 3D-графики с полноценной поддержкой технологий виртуализации графических адаптеров NVIDIA GRID и AMD MxGPU.

В качестве гостевых ОС поддерживаются стандартные дистрибутивы Linux и Microsoft Windows. Также поддерживаются российские операционные системы ROSA Linux, ALT Linux, Astra Linux, «РЕД ОС».

Платформа включена в Единый реестр российского ПО.

Требования к безопасности

Регулирующий орган в сфере информационной безопасности в России – ФСТЭК. Поэтому при организации мер защиты большинство производителей платформ виртуализации и заказчиков ориентируются на приказы и рекомендации этого ведомства. Наличие у продукта сертификата ФСТЭК является определяющим преимуществом для систем виртуализации на предприятиях, являющихся субъектами КИИ (Критическая информационная инфраструктура).

ФСТЭК требует наличия следующих функций безопасности в среде виртуализации:

- доверенная загрузка виртуальных машин – средство виртуализации должно блокировать запуск виртуальной машины при выявлении нарушения целостности конфигурации виртуального оборудования;
- контроль целостности – средство виртуализации должно контролировать целостность в процессе загрузки и динамически в процессе функционирования, информировать администратора безопасности о нарушении целостности, контролировать целостность конфигурации виртуального оборудования виртуальных машин и контролировать целостность исполняемых файлов и параметров настройки средства виртуализации;
- регистрация событий безопасности – средство виртуализации должно обеспечивать регистрацию событий безопасности, связанных с функционированием средства виртуализации. Оповещать администратора безопасности о событиях безопасности, осуществлять сбор и хранение записей в журнале событий безопасности;
- управление доступом – в средстве виртуализации должен быть реализован ролевой метод управления доступом с четырьмя ролями пользователей: разработчик виртуальной машины, администратор безопасности средства виртуализации, администратор средства виртуализации, администратор виртуальной машины;
- резервное копирование – средство виртуализации должно обеспечивать резервное копирование образов виртуальных машин, конфигурации виртуального оборудования виртуальных машин и сведений о событиях безопасности самостоятельно или с применением хостовой операционной системы или сертифицированных средств резервного копирования;
- управление потоками информации – средство виртуализации должно обеспечивать управление потоками информации между виртуальными машинами и информационными (автоматизированными) системами на канальном и сетевом уровнях самостоятельно или с применением сертифицированных средств управления потоками информации;
- защита памяти – средство виртуализации должно очищать остаточную информацию в памяти средства вычислительной техники при ее освобождении (распределении) или блокирование доступа субъектов к остаточной информации. Удалять объекты файловой системы путем перезаписи уничтожаемых (стираемых) объектов. Размещать код средства виртуализации в области памяти, недоступной одновременно для записи и исполнения. Изолировать области памяти виртуальных машин;
- ограничение программной среды – средство виртуализации должно осуществлять контроль за запуском компонентов программного обеспечения для выявления и блокировки запуска компонентов программного обеспечения, не включенных в перечень (список) компонентов, разрешенных для запуска;
- идентификация и аутентификация пользователей – первичная идентификация пользователей

средства виртуализации должна осуществляться администратором средства виртуализации; в случае неуспешной идентификации и аутентификации пользователей их попытка доступа должна быть заблокирована; средство виртуализации должно осуществлять аутентификацию пользователей при предъявлении идентификатора и пароля пользователя; у пользователя должна быть возможность смены пароля; не должно быть возможности установки одинаковых паролей для разных пользователей; аутентификационная информация должна храниться в защищенном виде;

- централизованное управление образами виртуальных машин и виртуальными машинами – средство виртуализации должно создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе; обеспечивать чтение записей о событиях безопасности; формировать отчеты по заданным критериям; делать выгрузку (экспорт) данных из журнала событий безопасности средства виртуализации и обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.

Все эти требования направлены на обеспечение безопасности приложений, выполняемых в среде виртуализации. Они обеспечивают достоверность выполняемого кода, изолируют приложения друг от друга, ограничивают несанкционированный доступ к приложениям, регистрируют события, относящиеся к безопасности, и защищают хранимые и передаваемые данные в среде виртуализации.

Перечисленные требования не уникальны и придуманы не сегодня. По большей части это переработка лучших зарубежных практик защиты информации, изложенных в документах Red Hat Enterprise Linux Virtualization Security Guide и CIS VMware ESXi Benchmark.

Сравнение аналогов

Популярная зарубежная платформа VMware является гипервизором первого типа, т. е. устанавливается на «железо» (bare metal), без промежуточной операционной системы общего назначения. Большинство отечественных систем виртуализации построены на Kernel-based Virtual Machine (KVM), что является частью ядра linux. Соответственно, это гипервизоры второго типа со всеми вытекающими возможностями.

При сравнении отечественных систем виртуализации с зарубежными можно уверенно сказать, что все базовые функции выполняются хорошо. За последние два года отечественные системы достигли высокого уровня зрелости.

К преимуществам отечественных систем можно отнести русскоязычный графический интерфейс, все инструкции, как и поддержка, на русском языке. Стоимость решений сравнить трудно, поскольку зарубежные вендоры покинули наш рынок.

> Для компаний с полным или частичным государственным участием должно закупаться только ПО, внесенное в реестр российского программного обеспечения.

В числе недостатков – высокая трудоемкость администрирования. Часто приходится заглядывать в консоль управления и выполнять многие процедуры вручную. Требуются хорошие знания Linux. Специалист должен хорошо представлять, что и как работает «под капотом».

Правительство регулирует использование отечественного ПО на уровне законодательства. Для компаний с полным или частичным государственным участием должно закупаться только ПО, внесенное в реестр российского программного обеспечения.

Постановление Правительства РФ № 1478 обязывает использовать на объектах критической информационной инфраструктуры (КИИ) только программное обеспечение, получившее сертификат ФСТЭК.

В поисках оптимального решения

Один из наиболее сложных и многогранных вопросов – по каким критериям следует выбирать оптимальное для предприятия или компании решение. В этот перечень входит множество факторов: и требуемая производительность платформы, и квалификация обслуживающего персонала предприятия, и возможность приобретения аппаратного обеспечения в виде серверов, систем хранения и передачи данных.

Наряду с этим следует учитывать нюансы, связанные с размещением оборудования, серверными помещениями, энергоснабжением, отводом выделяемого тепла. Большую роль, безусловно, играют цена, расходы на сопровождение, т. е. стоимость владения программно-аппаратным комплексом. Одна из ключевых рекомендаций – обратиться с запросом в профильную компанию-интегратор, чтобы аргументированно сравнивать представленные на рынке решения и соотнести их возможности с запросами конкретного предприятия или организации. ■