DOI: 10.22184/1992-4178.2018.180.9.84.90

Отечественная защищенная платформа виртуализации «Горизонт-ВС»

И. Коптелов[1], С. Назаров, д. т. н.[2], М. Ермолова[3]

УДК 004.946 | ВАК 05.13.00

Одна из задач импортозамещения – содействие переходу ключевых компаний и госорганов на отечественное программное обеспечение. Постановлением Правительства РФ № 1236 от 20 декабря 2017 года установлен запрет на использование и закупку импортного ПО для государственных и муниципальных нужд. Важную роль в построении современной ИТ-инфраструктуры госорганов и компаний занимает ПО систем виртуализации. С его помощью создается виртуальная инфраструктура – комплекс систем на основе виртуальных машин, обеспечивающих предприятия новыми возможностями при сохранении существующей схемы использования ИТ-ресурсов. Рассмотрим порядок построения виртуальных сред на примере наиболее распространенного ПО импортного и отечественного производства, представим архитектуру и межмодульное взаимодействие отечественной платформы виртуализации «Горизонт-ВС», а также результаты ее тестирования.

ВВЕДЕНИЕ

Сегодня виртуализация – базовая инфраструктурная технология. Классификация технологий виртуализации связана с возможностями программ-гипервизоров. По сути, гипервизор – это расширенное и обобщенное понятие супервизора. Супервизор в ядре ОС обеспечивает изоляцию пользовательских программ друг от друга, выделение и освобождение ресурсов для пользовательских процессов, а гипервизор – изоляцию и управление ресурсами для самих ОС как целого, вместе с их пользователями и процессами.

В реализации технологий виртуальных машин (ВМ) можно выделить три основных подхода [1–3]:

1. гипервизор первого типа – минимальная операционная система, исполняемая непосредственно на аппаратном уровне компьютера, выполняющая функции эмуляции физического аппаратного обеспечения, управления аппаратными средствами и гостевыми ОС;
2. гипервизор второго типа (хостовый, монитор виртуальных машин) – дополнительный программный слой поверх основной хостовой ОС, который выполняет функции управления гостевыми ОС, а эмуляцию и управление аппаратурой берет на себя хостовая ОС;
3. гибридный гипервизор – комбинированный вариант первых двух, управление аппаратными средствами выполняется тонким гипервизором и специальной сервисной ОС, работающей под управлением тонкого гипервизора.

Обычно гипервизор управляет напрямую процессором и памятью компьютера, а гостевые ОС работают с остальными аппаратными компонентами через сервисную ОС. Гипервизор первого типа, впервые реализованный компанией IBM в 1960 году в виде системы CP/CMS [4, 5], считается классическим вариантом архитектуры ВМ. В настоящее время виртуализация ИТ-инфраструктуры активно внедряется многими ведущими компаниями – системными интеграторами, которые являются авторизованными партнерами провайдеров систем виртуализации. В процессе виртуализации ИТ-инфраструктуры создается виртуальная инфраструктура – комплекс систем на основе виртуальных машин, обеспечивающих функционирование всей ИТ-инфраструктуры, обладающий многими новыми возможностями при сохранении существующей схемы деятельности ИТ-ресурсов. Основой ИТ-инфраструктуры является кластер – разновидность параллельной или распределенной системы, которая состоит из нескольких связанных компьютеров, используемых как единый, унифицированный компьютерный ресурс.

[1] ООО «Инновационный Центр «Баррикады», и.о. генерального директора, koptelov@gorizont-vs.ru, igor.koptelov@mail.ru.

[2] ЗАО «МНИТИ», главный специалист, профессор, действительный член Международной академии информатизации, nazarov@mniti.ru, s_nazarov@mail.ru.

[3] ООО «Инновационный Центр «Баррикады», исполнительный директор, ассистент МГТУ им. Н. Э. Баумана, ermolova@gorizont-vs.ru, ermolova.88@mail.ru.

В корпоративной сети и виртуальных средах кластеры высокой доступности традиционно применяются для обеспечения непрерывной работы приложений в режиме 24/7/365 с минимальным временем простоя и гибкой масштабируемости сети по требуемому уровню нагрузки. Развитие виртуальных ИТ-инфраструктур предусматривает создание конвергентных инфраструктур, объединяющих вычислительные, сетевые ресурсы, систему хранения данных и администрирование ИТ в предварительно настроенном пакете, которым можно управлять как единой системой.

Ведущими производителями в этой области являются VMWare, Microsoft, Citrix и RedHat, разработавшие целый ряд семейств коммерческих продуктов для создания виртуальной среды [6–8]. Однако все они – зарубежные компании, использование их продукции не соответствует государственной политике импортозамещения и концепции обеспечения национальной информационной безопасности. Среди отечественных аналогов можно отметить «Горизонт-ВС», ПК «Виртуализации и управления» и ПК «Брест», имеющие сертификаты соответствия, полученные от систем сертификации средств защиты информации по требованиям безопасности информации [9].

ПК «Виртуализации и управления» и ПК «Брест» – гипервизоры второго типа, поскольку предназначены для функционирования под управлением операционной системы специального назначения (ОССН) Astra Linux Special Edition, релиз «Смоленск» (аппаратная платформа x86–64), используют модули ядра для KVM непосредственно из состава ОССН [10]. Функций по созданию замкнутой программной среды названные программные комплексы непосредственно не реализуют – используют соответствующие механизмы ОССН.

Платформа «Горизонт-ВС» – гипервизор первого типа (устанавливается непосредственно на аппаратную платформу). В платформе реализован механизм создания замкнутой программной среды, работающий на основе модулей специализированной сборки ядра Linux.

АРХИТЕКТУРА ПЛАТФОРМЫ ВИРТУАЛИЗАЦИИ «ГОРИЗОНТ-ВС»

Платформа «Горизонт-ВС» представляет собой встроенное программное обеспечение, состоящее из пространства ядра и пользовательского пространства. Основой «Горизонт-ВС» является гипервизор, включающий в себя модуль KVM и эмулятор аппаратного окружения виртуальных машин QEMU [11]. Гипервизор предоставляет нескольким гостевым ОС, работающим под его управлением на одном вычислителе, средства связи и взаимодействия между собой (например, через обмен файлами или сетевые соединения) так, как если бы эти ОС выполнялись на разных физических компьютерах. Функции системного управления гипервизором QEMU/KVM выполняет компонент libvirt [12] – кроссплатформенная библиотека управления виртуализацией на основе различных гипервизоров, в том числе KVM и QEMU, позволяющая контролировать по сети виртуальные машины на других компьютерах.

Совместно с libvirt используется менеджер виртуальных машин virt-manager, предоставляющий графический и консольный интерфейс для создания и контроля состояния виртуальных машин на уровне отдельных серверов и ВМ. Менеджер виртуальных машин также предоставляет возможность управления удаленным сервером виртуализации, осуществляет сетевое соединение с удаленным процессом libvirtd из состава библиотеки libvirt. Сервис libvirtd способен создавать требуемые ВМ и подключать к ним необходимые ресурсы.

Пользовательское пространство в «Горизонт-ВС» представлено модулем virt-manager, реализующим графический интерфейс управления на уровне отдельных серверов и ВМ, и веб-интерфейсом. Модуль virt-manager совместно с веб-интерфейсом позволяет управлять всеми виртуальными подсистемами изделия через функции управления системного уровня libvirt. Сетевая виртуальная среда «Горизонт-ВС» реализована на основе модуля bridge-utils. Системное управление этими компонентами обеспечивается средствами libvirt. Схема взаимодействия модулей «Горизонт-ВС» представлена на рис. 1.

Модуль KVM (Kernel-based Virtual Machine) обеспечивает аппаратную виртуализацию на базе процессоров Intel-VT либо AMD SVM. ПО KVM состоит из загружаемого модуля ядра, предоставляющего базовый сервис виртуализации, процессорно-специфического загружаемого модуля, использующего возможности конкретного процессора, и компонентов пользовательского режима. Загрузка вышеперечисленных модулей превращает ядро в гипервизор. В архитектуре гипервизора «Горизонт-ВС» виртуальная машина исполняется как обычный процесс, что позволяет задействовать все возможности ядра.

Модуль ядра поддерживает динамическую миграцию, обеспечивая возможность перемещения работающих виртуальных машин между физическими узлами без прерывания обслуживания. Динамическая миграция прозрачна для пользователей: виртуальная машина остается включенной, сетевые соединения активными, пользовательские приложения продолжают работать, в то время как виртуальная машина перемещается на новый физический сервер. Наряду с динамической миграцией гипервизор поддерживает сохранение копии текущего состояния виртуальной машины на диск, позволяя хранить ее и восстанавливать позднее.

Модуль QEMU обеспечивает виртуальное аппаратное окружение для гостевых ОС: BIOS, шины PCI, шины USB, а также стандартный набор устройств, таких как дисковые контроллеры IDE и SCSI, сетевые карты

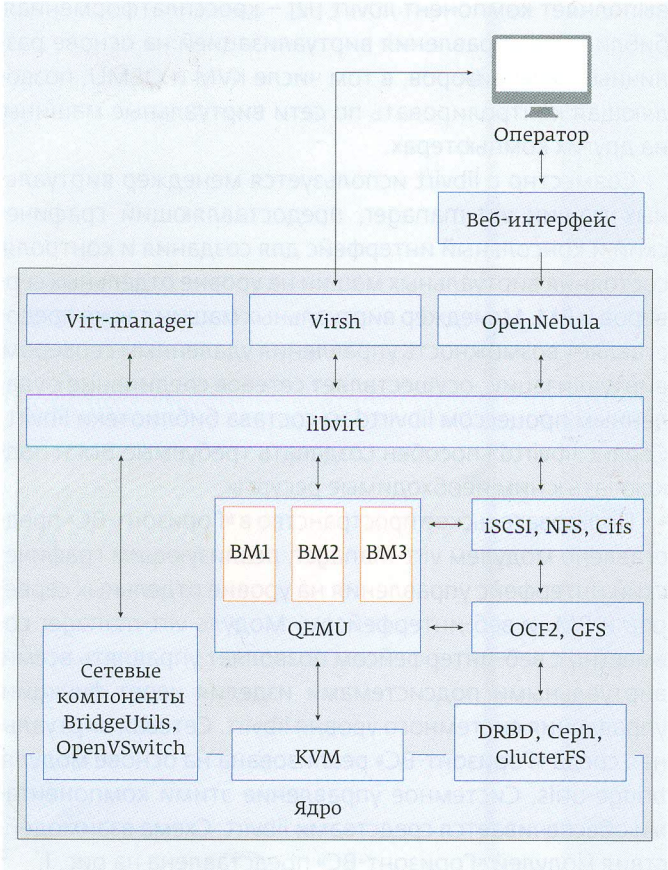

Рис. 1. Архитектура гипервизора «Горизонт-ВС»

и т. д. В гипервизоре «Горизонт-ВС» виртуальные машины в окружении QEMU исполняются как процесс от имени назначенного пользователя. QEMU в качестве эмулятора виртуальной машины может обеспечивать запуск ОС и программ, разработанных для одной аппаратной платформы (например, ARM или MIPS) на аппаратных платформах другого типа (например, на x86-совместимой).

Таким образом, полноценным гипервизор становится только при совместном функционировании модуля ядра с QEMU, эмулирующим устройства ввода-вывода и BIOS. Модуль QEMU в режиме виртуализации выполняет гостевой код непосредственно на центральном процессоре, благодаря чему достигается производительность, близкая к производительности хостовой системы.

Для каждой виртуальной машины запускается отдельный процесс QEMU. При выключении гостевой системы этот процесс уничтожается или осуществляется выход из него. Помимо потоков виртуальных процессоров существуют специализированные потоки, в которых обрабатываются операции ввода-вывода, такие как передача сетевых пакетов и дисковые операции.

Каждая ВМ функционирует как изолированный процесс в пространстве пользователя. Программный интерфейс работы с памятью эмулирует пространство оперативной памяти, шины и контроллеры ввода-вывода QEMU и позволяет эмулировать:

- обычную память;
- отображение в память ввода-вывода (MMIO);
- контроллеры памяти, которые могут динамически перенаправлять регионы физической памяти к различным адресатам.

Взаимодействие с интерфейсом пользователя осуществляется через системную библиотеку. Функции взаимодействия с различными объектами в libvirt реализованы в драйверах – программных модулях, которые в момент инициализации регистрируются libvirt. Каждый драйвер регистрирует API-функции, реализованные на API-интерфейсах libvirt.

Внутренние поля структуры определяют, какой тип драйвера представлен каждым из членов поля. Драйверы классифицируются как драйверы первого и второго уровня. Драйвер гипервизора – первого уровня. В состав драйверов второго уровня входят:

- управление свойствами виртуального процессора;
- управление сетевыми интерфейсами хоста;
- управление виртуальными сетями и NAT;
- управление перечнем хостовых устройств;
- управление доступом к виртуальным машинам, реализующее политику дискреционного доступа;
- управление дисковыми системами.

Libvirt порождает процесс QEMU-KVM, который взаимодействует с модулями ядра. QEMU взаимодействует с KVM через различные вызовы. При создании виртуальной машины libvirt порождает процесс QEMU, который, в свою очередь, создает виртуальную машину. Для каждой виртуальной машины сервисом libvirtd запускается отдельный процесс QEMU-KVM. Свойства виртуальных машин (количество процессоров, объем памяти, конфигурация устройств ввода-вывода) описываются в отдельных XML-файлах, используемых сервисом libvirtd для формирования списка аргументов, который передается в виде командной строки при запуске процесса QEMU-KVM.

В платформе «Горизонт-ВС» реализован отказоустойчивый кластер, основанный на ПО с открытым исходным кодом Pacemaker и Corosync [13]. Для создания кластерного хранилища с числом хостов, равным двум, применяется подход создания реплицируемого блочного устройства DRBD. Для построения кластерного хранилища с числом хостов больше двух применяется подход создания реплицируемого блочного устройства либо распределенной файловой системы средствами сети хранения Ceph [14].

В качестве интерфейса управления средствами среды виртуализации на единичном сервере виртуализации используется модуль virt-manager с функциями поддержки модели дискреционного и мандатного разграничения прав доступа. В окне графического интерфейса администратору доступно поле для назначения ВМ пользователя, имеющего к ней доступ, а также установки уровня

доступа ВМ к файлам на общем хранилище. После сохранения настроек ВМ будет запускаться от его имени и с его правами.

Система группового управления платформой «Горизонт-ВС» – высокоуровневое средство управления облачной инфраструктурой через веб-интерфейс – состоит из следующих подсистем:

- управления пользователями и группами;
- управления виртуализацией;
- управления хостами;
- мониторинга показателей доступности, производительности и степени загруженности, контролируемых виртуальных и физических ресурсов;
- сбора статистики;
- управления виртуальными сетями;
- управления хранилищами;
- обеспечения высокой доступности;
- кластерной подсистемы;
- создания и управления зонами;
- организации виртуального изолированного облака;
- безопасности.

Подсистема безопасности логически разделена на несколько подсистем:

- аутентификации и авторизации пользователей;
- управления списками контроля доступа;
- обеспечения изоляции ресурсов на различных уровнях.

На рис. 2 и 3 представлен ряд интерфейсов системы группового управления.

Администратору, управляющему виртуальной инфраструктурой через веб-интерфейс, предоставляются следующие возможности:

- динамическое изменение размера физической инфраструктуры путем добавления или удаления узлов и разбиения кластера на виртуальные разделы, позволяющие выделять необходимый объем ресурсов для функционирования определенного сервиса;

Рис. 2. Информационная панель

- централизованный интерфейс для управления всеми элементами виртуальной и физической распределенной инфраструктуры;
- высокая степень задействования доступных ресурсов, возможность подключения внешних ресурсов или организации совместного использования инфраструктуры между несколькими подразделениями;

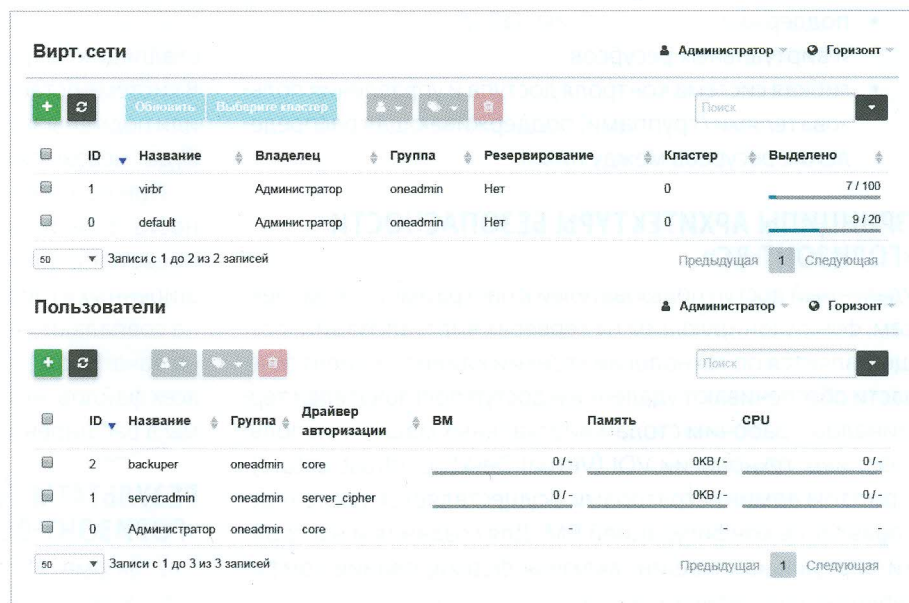

Рис. 3. Интерфейсы системы группового управления

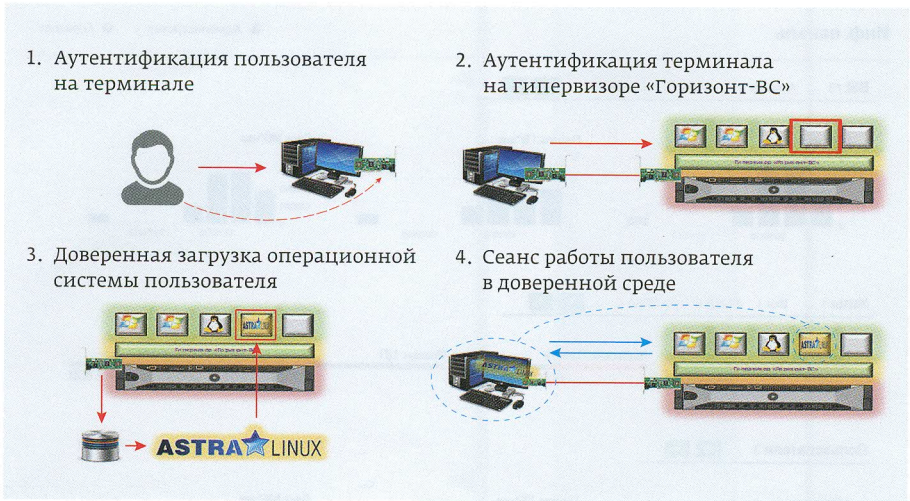

Рис. 4. Процесс аутентификации в «Горизонт-ВС»

- сокращение издержек за счет уменьшения числа физических серверов, снижение затрат на администрирование, обслуживание, энергоснабжение и охлаждение;
- быстрого наращивания серверной мощности за счет подключения ресурсов внешних облачных сервисов в моменты пиковой нагрузки;
- механизмы обеспечения отказоустойчивости: реализована функция автоматического выполнения операций по восстановлению работоспособности окружений в случае сбоя в работе физического сервера или виртуальной машины;
- поддержка управления квотами путем задания определенным пользователям набора ограничений на использование ресурсов;
- поддержка групп со своим набором пользователей и виртуальных ресурсов;
- гибкая система контроля доступа и управления пользователями / группами, поддерживающая распределение ресурсов между ними.

ПРИНЦИПЫ АРХИТЕКТУРЫ БЕЗОПАСНОСТИ «ГОРИЗОНТ-ВС»

Удаленный доступ пользователей к программным комплексам, функционирующим на серверах виртуализации, осуществляется по технологии «тонкий клиент». Клиентские части обеспечивают удаленный доступ пользователей терминалов к рабочим столам виртуальных машин с использованием технологии VDI (Virtual Desktop Infrastructure). При этом администраторами осуществляется удаленное управление конфигурацией ВМ. Для создания и настройки виртуальных машин, включая формирование конфигурации аппаратных средств ВМ, установку гостевых ОС в ВМ и прочие функции управления, используются консольные или графические средства.

После прохождения процедуры идентификации и аутентификации пользователи запускают виртуальную машину либо с использованием технологии VDI по протоколам VNC и SPICE, получают доступ к ранее запущенным виртуальным машинам в соответствии с установленными правилами разграничения доступа. Запущенная виртуальная машина представляет собой процесс в операционной среде вычислительного узла, который функционирует от имени учетной записи пользователя с его мандатными и дискреционными атрибутами безопасности (рис. 4).

Для контроля действий пользователей, особенно наделенных административными полномочиями, используется система аудита с функцией протоколирования фактов несанкционированного доступа / нарушений модели безопасности в реальном времени. В платформе виртуализации реализована очистка оперативной и внешней памяти, осуществляемая при ее освобождении и перераспределении путем записи случайной последовательности.

В системе «Горизонт-ВС» реализована изолированная программная среда. В процессе инициализации системы автоматически генерируется пара ключей – закрытый и открытый. Для всех без исключения инсталлируемых на жесткий диск файлов «Горизонт-ВС» автоматически подсчитывается хеш-сумма, которая подписывается сгенерированным закрытым ключом. Подписанная хеш-сумма сохраняется в расширенных атрибутах файловой системы для каждого файла в отдельности. После завершения инсталляции закрытый ключ автоматически уничтожается. В системе остается открытый ключ, в случае его удаления или подмены загрузка и функционирование «Горизонт-ВС» будет невозможна.

При попытке доступа к файлу проверяется его целостность, то есть подсчитывается хеш-сумма файла и сравнивается с сохраненной в процессе инсталляции в расширенных атрибутах файловой системы. Если хеш-суммы не совпадают, запуск файла блокируется ядром системы на начальном этапе загрузки. Также заблокирован запуск всех файлов, не имеющих подписанной контрольной суммы в расширенных атрибутах.

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ ПЛАТФОРМЫ «ГОРИЗОНТ-ВС»

Платформа «Горизонт-ВС» прошла ряд нагрузочных и функциональных тестирований.

В Центре обработки данных (ЦОД) на территории компании ОАО «КОМКОР» (Варшавское шоссе, д. 133)

в период с 4 по 11 августа 2016 года и с 28 сентября по 3 октября 2016 года проводилось сравнительное тестирование производительности гипервизоров XEN, KVM и VMWare 6.0.0. Для этого использовались серверы производства компании Huawei RH2288h V3 с техническими характеристиками, приведенными в таблице.

Программное обеспечение – гипервизоры «Горизонт-ВС» на основе модифицированного гипервизорного модуля KVM, VMWare 6.0.0 на основе проприетарного гипервизорного модуля VMware ESXi и Huawei FusionSPhere на основе гипервизора Xen – было развернуто на трех идентичных аппаратных платформах (каждый гипервизор на отдельной платформе).

Тестирование производительности проводилось с использованием программного обеспечения, установленного на ВМ «Сервер» и «Клиент», имитирующего работу высоконагруженных банковских систем обработки платежной информации. На каждой ВМ «Клиент» были автоматически созданы 100 000 входящих файлов, подписанных ЭЦП и зашифрованных блочным шифром. На всех ВМ «Клиент» одновременно запускался тест. Входные файлы последовательно расшифровывались, проверялась ЭЦП, зашифровывались, переподписывались и сохранялись на дисковой системе. Результаты обработки сохранялись на ВМ «Сервер» в текстовом файле.

Результаты тестирования:

- время теста (время обработки всех входных файлов);
- скорость теста (количество обработанных входных файлов в секунду);
- суммарная производительность (общее количество файлов, обработанных всеми ВМ за 1 с).

На рис. 5–7 в графическом виде обобщены результаты тестирования.

Тесты показали, что количество обработанных за 1 с файлов в виртуальных машинах, функционирующих под управлением «Горизонт-ВС», выше в среднем на 20%, чем у ВМ под управлением других гипервизоров. Таким образом, виртуальная среда «Горизонт-ВС» эффективнее как на вычислительных, так и на дисковых операциях.

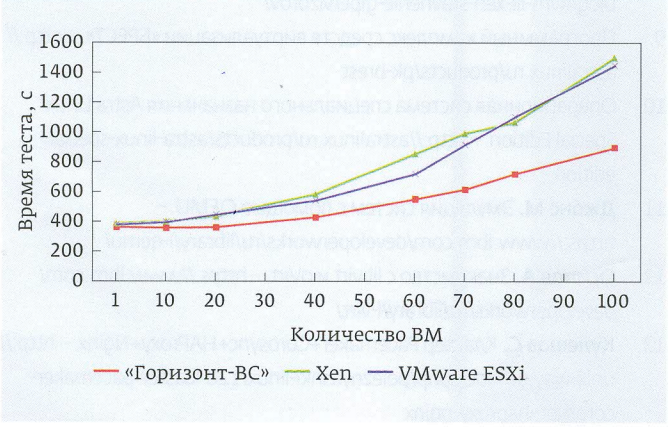

Рис. 5. График времени обработки файлов

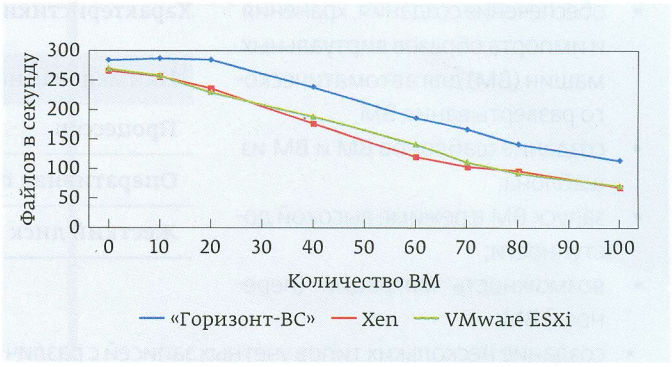

Рис. 6. График скорости теста

В июне 2018 года оценивались функциональные возможности платформы виртуализации «Горизонт-ВС» на базе ЦОД Минобороны России. Представители Главного управления развития информационных и телекоммуникационных технологий Минобороны России (ГУРИТТ МО РФ) и 27-го Центрального научно-исследовательского института Министерства обороны Российской Федерации убедились в полном соответствии платформы «Горизонт-ВС» заявленному функционалу:

- доступ к системе группового управления через веб-браузер;
- возможность подключения узлов к СГУ и объединения их в кластер;
- вывод в интерфейс управления информации о текущем состоянии, доступности каждого вычислительного узла;
- обеспечение создания и управления виртуальной инфраструктурой как на серверной платформе, так и на группе серверных платформ (кластер);
- возможность добавления вычислительных узлов в кластер, а также их удаления без необходимости переконфигурации (первоначальной настройки) виртуальной инфраструктуры;

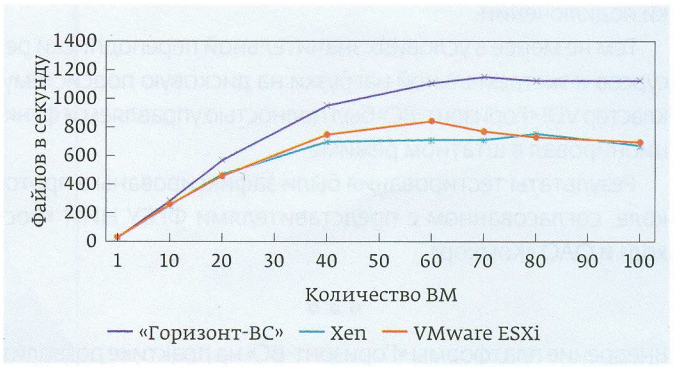

Рис. 7. График производительности гипервизоров

- обеспечение создания, хранения и импорта образов виртуальных машин (ВМ) для автоматического развертывания ВМ;
- создание шаблонов ВМ и ВМ из шаблона;
- запуск ВМ в режиме высокой доступности;
- возможность миграции (переноса) ВМ;
- создание нескольких типов учетных записей с различным уровнем привилегий на основе мандатного и дискреционного управления доступом.

Положительные результаты тестирования зафиксированы в протоколе и акте, утвержденных начальником ГУ РИТТ МО РФ.

В августе 2018 года в ЦОД на территории компании ОАО «КОМКОР» проводилось нагрузочное стресс-тестирование гиперконвергентного VDI-решения «Горизонт-ВС». На стенде использовалось серверное оборудование компании Huawei RH2288h V3. На пяти идентичных серверах с развернутым программным обеспечением «Горизонт-ВС» было инсталлировано две тысячи виртуальных машин со следующими параметрами:

- «гостевая» ВМ (в количестве 1000 ВМ): 1 vCPU, 1024 Мбит ОЗУ, гостевая ОС Fedora 25;
- «тонкий клиент «Горизонт-ВС» (в количестве 1000 ВМ): 1 vCPU, 256 Мбит ОЗУ, ПО «Тонкий клиент «Горизонт-ВС».

В ходе тестирования осуществлялся одновременный запуск «гостевых» ВМ и «тонких клиентов «Горизонт-ВС» в виртуальной среде «Горизонт-ВС». При запуске ВМ выполнялось автоматическое VDI-подключение ВМ «тонких клиентов «Горизонт-ВС» к «гостевым» ВМ с использованием диспетчера соединений «Горизонт-ВС». В результате тестирования выяснилось, что средства «Горизонт-ВС» обеспечивают равномерное распределение нагрузки между серверами. На тестовом стенде удалось запустить две тысячи виртуальных машин в условиях переподписки с коэффициентом более 1,5 и осуществить тысячу одновременных VDI-соединений с обеспечением равномерного распределения нагрузки подключений.

Тем не менее в условиях значительной переподписки ресурсов и экстремальной нагрузки на дисковую подсистему кластер VDI «Горизонт-ВС» был полностью управляем и функционировал в штатном режиме.

Результаты тестирования были зафиксированы в протоколе, согласованном с представителями ФГБУ НИИ «Восход» и ОАО «Комкор».

* * *

Внедрение платформы «Горизонт-ВС» на практике позволит организовать комплексную защиту данных и операций, осуществляемых в виртуальных средах. Решение обеспечивает надежную среду исполнения виртуальных машин, подключение к ним терминалов на сервере виртуализации с использованием технологии VDI, а также предоставляет средства защиты исполняемых в виртуальном окружении операционных систем и ПО. Применение «Горизонт-ВС» позволит мигрировать с физических серверов на виртуальные, увеличив загрузку аппаратной платформы в несколько раз, что существенно повысит коэффициент использования аппаратуры. Еще одно преимущество – экономия на обслуживании серверов и потребляемой электроэнергии.

Характеристики оборудования

Наименование	Модель	Количество, шт.
Процессор	Intel Xeon E5-2699 v3 2,3 ГГц	2
Оперативная память	Micron DIMM DDR416384 Мбит	20
Жесткий диск	HDD SAS2 Тбит	12

ЛИТЕРАТУРА

1. **Рудь И.** Битва гипервизоров: VMware vs Hyper-V. – http://itband.ru/
2. **Пастухов Д.А., Юрчик П.Ф., Остроух А.В.** Сравнительный анализ гипервизоров. – https://expeducation.ru/ru/article/view?id=7145
3. **Рубанов В.** Серверная виртуализация: гипервизоры против контейнеров. Журнал сетевых решений/LAN. 2017. № 01–02. – https://www.osp.ru/lan/2017/01–02/13051363/
4. Виртуализация: история и тренды развития. – https://habr.com/company/1cloud/blog/237005/
5. Решения виртуализации от IBM и HP. – https://www.ibm.com/developerworks/ru/library/au-aixhpvirtualization/
6. Войны гипервизоров: To be continued. – https://habr.com/company/cloud4y/blog/310002/
7. Сравнение гипервизоров Hyper-V, XenServer и vSphere. – https://www.excloud.by/article/sravnenie-gipervizorov-hyper-v-xenserver-i-vsphere/
8. KVM или Xen – сравнение гипервизоров. – https://adminvps.ru/blog/kvm-ili-xen-sravnenie-gipervizorov/
9. Программный комплекс средств виртуализации «БРЕСТ». – http://astralinux.ru/products/pk-brest
10. Операционная система специального назначения Astra Linux Special Edition. – http://astralinux.ru/products/astra-linux-special-edition
11. **Джонс М.** Эмуляция систем с помощью QEMU. – https://www.ibm.com/developerworks/ru/library/l-qemu/
12. **Осипов А.** Знакомство с libvirt и oVirt. – https://www.ibm.com/developerworks/ru/library/l-virt/
13. **Кулешов С.** Кластер Pacemaker+Corosync+HAProxy+Nginx. – http://unix-way.ru/index.php/poleznyashki-linux/120-klaster-pacemaker-corosync-haproxy-nginx
14. **Сингх К.** Изучаем Ceph. – http://support.mdl.ru/learningceph/content/index.html#Copyright