Bitdefender®

The impact of virtualization security on your VDI environment

Оглавление

Введение

Виртуализация (использование виртуальных объектов) обеспечивает организациям значительную экономию средств и гибкость бизнеса. Одна из технологий виртуализации, которой пользуется большинство организаций, называется инфраструктурой виртуальных рабочих столов (VDI). VDI дает работникам и работодателям ряд преимуществ, независимо от размера организации. Одним из преимуществ VDI является возможность предоставлять централизованно управляемую среду рабочих столов сотрудникам на любом устройстве. Используя эту технологию, организация может быть уверена, что доступ к информации и управление ею будут всегда безопасными, независимо от того, откуда пользователь получает доступ к этой информации.

VDI требуется не всем. Тем не менее, она полезна в производственных сферах, таких как центры обработки вызовов, которые имеют высокую концентрацию работников, ориентированных на определенные задачи, или заменяет крупномасштабные развертывания настольных систем на базе офиса. Однако, как и в любой среде, безопасность всегда должна играть ключевую роль и дополнять бизнес-среду. Это полностью реализуется с VDI; безопасность должна быть беспрепятственной, без какого-либо влияния на работу пользователя. Предназначенная для физических сред, традиционная система безопасности может затруднить развертывание VDI, что полностью меняет цель использования виртуализации или VDI, состоящей, прежде всего, – в эффективности, гибкости и экономии затрат.

В этом документе подробно описывается тестирование производительности, проводимое за счет использования стандартных инструментов, таких как Login VSI (подключение к VSI). Результаты теста показывают сравнение четырех решений по безопасности, доступных на рынке сегодня, которые были специально разработаны для виртуализированных сред. Приведенные результаты тестирования призваны помочь организациям лучше понять требование по масштабированию и ожидаемую производительность, которую они получат от развертывания в VDI с оптимизированной безопасностью виртуализации.

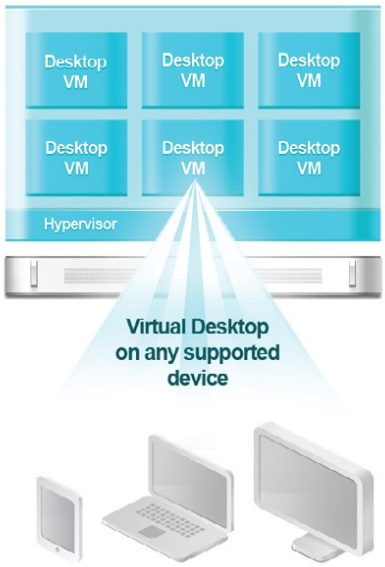

Рисунок 1: Инфраструктура виртуального рабочего стола

Что такое VDI?

Инфраструктура виртуальных рабочих столов (VDI) это практика, за счет которой операционная система настольных компьютеров размещается в виртуальной машине. Виртуальная машина может быть размещена в центре обработки данных организации или в облаке, в качестве службы (DaaS). При этом доступ к VDI можно получить с таких устройств, как тонкие клиенты, восстановленные ПК, смартфоны, планшеты и т. д. Это дает организациям возможность гарантировать качество взаимодействия с конечным пользователем независимо от устройства, используемого для подключения к корпоративной сети.

Проблемы безопасности виртуализации

Это общеизвестный факт, что программное обеспечение для защиты от вредоносных программ является неотъемлемым требованием безопасности на сегодняшний день. При этом пользователь может работать с приложениями и операционными системами, функционирующими в физических, виртуальных или облачных средах. Хотя в виртуализированных средах могут использоваться традиционные системы по обеспечению безопасности, изначально они не рассчитаны и не оптимизированы для таких сред.

Использование традиционных антивирусных решений может привести к определенным проблемам в среде VDI, таким как:

- Низкие коэффициенты консолидации (совместной производительности) виртуальных машин
- Задержка загрузки ОС
- Конфликты со стороны антивирусных программ
- Устаревшие антивирусные программы (AV) на неактивных виртуальных машинах
- Общие проблемы управления

Коэффициенты консолидации страдают в результате использования традиционных средств обеспечения безопасности в виртуальных средах. Традиционная безопасность рассматривает каждую виртуальную машину на изолированной основе; она не предназначена для оценки всех экземпляров виртуальной машины в конкретной сети или группе. Все действия приложения и пользователя, выполняемые на экземпляре виртуальной машины, оцениваются агентом безопасности в операционной системе. Этот эффект изолированного хранилища создает значительное дублирование, от баз данных сигнатур до результатов сканирования по тем же файлам, что в конечном итоге создает проблему производительности, и впоследствии снижает коэффициенты консолидации виртуальных машин.

Задержка загрузки является результатом использования традиционного вредоносного ПО в виртуальных средах. Когда виртуальная машина запущена, решение по безопасности должно загрузить свои последние сигнатуры антивирусного ядра и последние обновления программного обеспечения. Один только этот процесс обновления может занять от 5 до 12 секунд, что создает возможное окно для несанкционированных действий.

Конфликты со стороны антивирусных программ (АВП) возникают, когда традиционные агенты решений по безопасности, установленные на каждой виртуальной машине, пытаются выполнить обновление или сканирование по расписанию одновременно. При этом центральный процессор, память и процессор ввода-вывода испытывают перегрузки, что приводит к снижению производительности виртуальной машины и, в некоторых случаях, к полному отказу базового компьютера (хоста).

Агенты защиты традиционных АВП, установленные на неактивных виртуальных машинах, могут обновляться только при запуске виртуальной машины, что приводит к проблемам с задержкой загрузки и потенциальным АВП-конфликтам, в результате чего виртуальная машина не будет защищена самыми последними файлами сигнатур ядра.

Управление традиционными решениями по безопасности может стать утомительным; что особенно актуально при развертывании в крупной компании. Каждый раз, когда устанавливается новый традиционный агент, он регистрируется в консоли управления безопасностью, для целей последующего администрирования. Когда виртуальная машина ликвидирована или неактивна, традиционный агент по-прежнему остается зарегистрированным в консоли безопасности, и единственный способ удалить эту запись – сделать это вручную. Что может стать рутинной, обыденной задачей, особенно для крупных организаций, где виртуальные машины постоянно перемещаются.

Выбор правильного решения для безопасности виртуализации

Bitdefender воспользовались Login VSI (подключение к VSI) для тестирования VDI совместно с семью (7) другими решениями по обеспечению безопасности (антивирусными программами) виртуализации, доступным на текущий момент на рынке. Результаты отражают влияние этих решений на среду VDI.

Login VSI это стандартный инструментарий для тестирования производительности VDI, имитирующий типичное поведение пользователя в средах VDI.

Этот инструментарий позволяет измерить общее время отклика нескольких определенных пользовательских операций, выполняемых в пределах рабочей нагрузки рабочего стола в цикле сценариев. В частности, здесь важно отметить два значения: базовый уровень (Baseline) и VSImax.

- VSImax — это максимальное количество сеансов VDI, допустимых на хосте до снижения производительности хоста и VDI.
- Базовый уровень — это измерение времени отклика определенных операций, выполняемых на рабочем столе в пределах рабочей нагрузки, при отсутствии нагрузки на систему, который измеряется в миллисекундах (мс).

Низкий базовый уровень указывает на более эффективное взаимодействие пользователя с VDI. При взаимодействии с экземпляром VDI, если время отклика слишком велико, идеальная связь, когда виртуальный рабочий стол ведет себя как локальный, недостижима. Очень большое время отклика напоминает работу с динамической веб-страницей, для обновления которой требуются длительные периоды времени.

Все эти измерения представляют то, что можно получить, работая с определенным стеком. В тестировании было использовано одинаковое оборудование, программное обеспечение для виртуализации и прочие факторы были одинаковыми для всех протестированных решений. Единственным элементом, изменяемым от теста к тесту, было решение по защите от вредоносных программ (антивирусная программа). Единственный способ добиться лучших результатов с помощью одного и того же программного стека – это увеличить его вычислительную мощность за счет увеличения финансовых расходов.

Обратите внимание, что решения Bitdefender, McAfee Multiplatform и Kaspersky Light Agent не используют VMware vShield Endpoint, тогда как все другие решения полагаются на него. Bitdefender включает интеграцию vShield для клиентов, желающих использовать его.

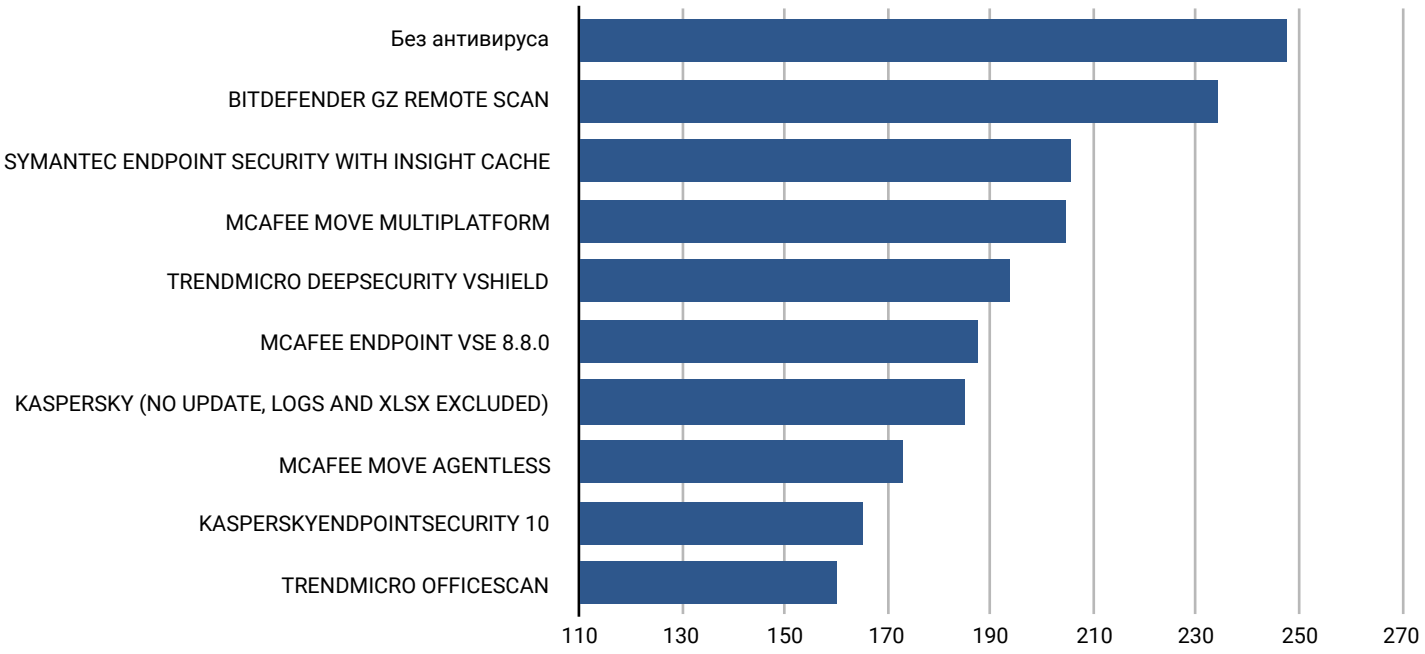

Рисунок 1: VSImax - максимально достижимое количество сеансов VDI

Рисунок 1 отображает VSImax каждого протестированного решения. Это самый простой тест, представляющий количество экземпляров VDI, которые можно запустить до того, как пользовательское приложение выйдет за пределы допустимого уровня (цифры на красной полосе). Хотя все тесты связаны с коэффициентами консолидации, этот тест представляет собой то, чего можно добиться в среде, даже с неидеальным пользовательским интерфейсом.

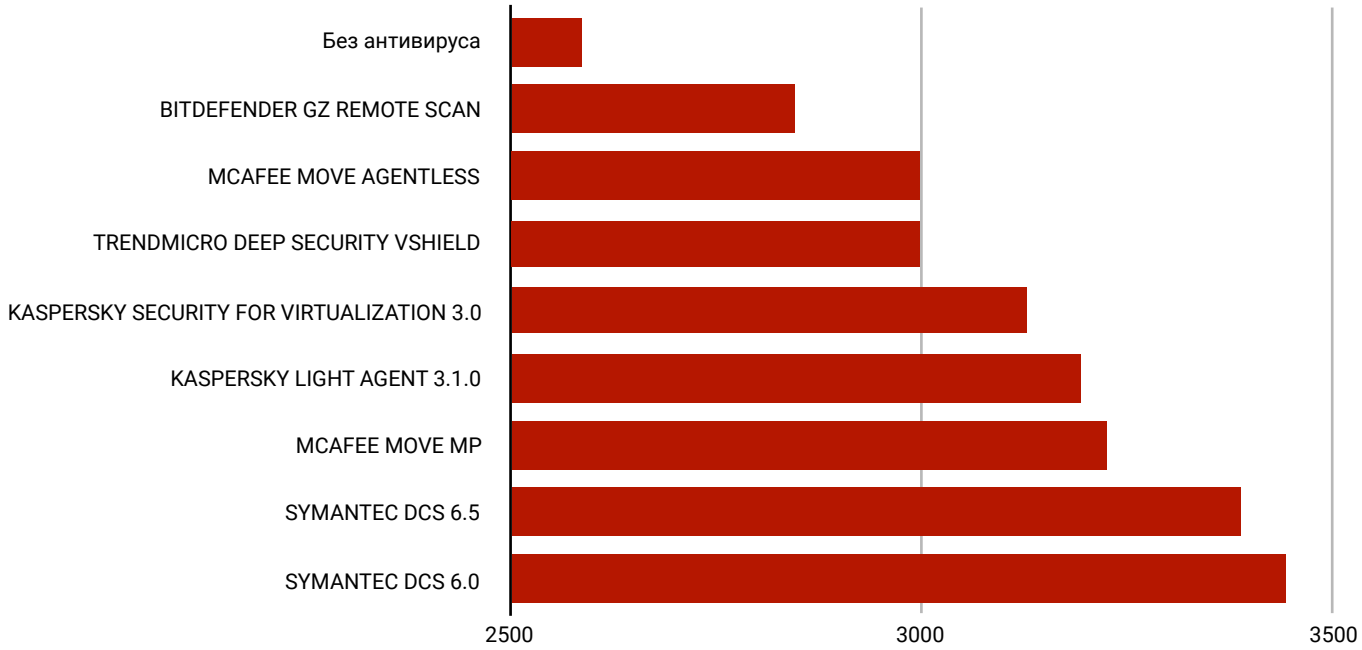

Рисунок 2: Базовый уровень, время отклика (мс) системы при рабочей нагрузке

На рисунке 2 представлены результаты теста на измерение базового уровня. Bitdefender дает наименьшее базовое время отклика, что обеспечивает лучшее взаимодействие с пользователем и высокую производительность при рабочей нагрузке (на компьютере пользователя), когда общая нагрузка на систему отсутствует.
По вертикальной оси указаны антивирусные программы, которые были протестированы в системе, по горизонтали время отклика операций, выполняемых пользователем, в миллисекундах.

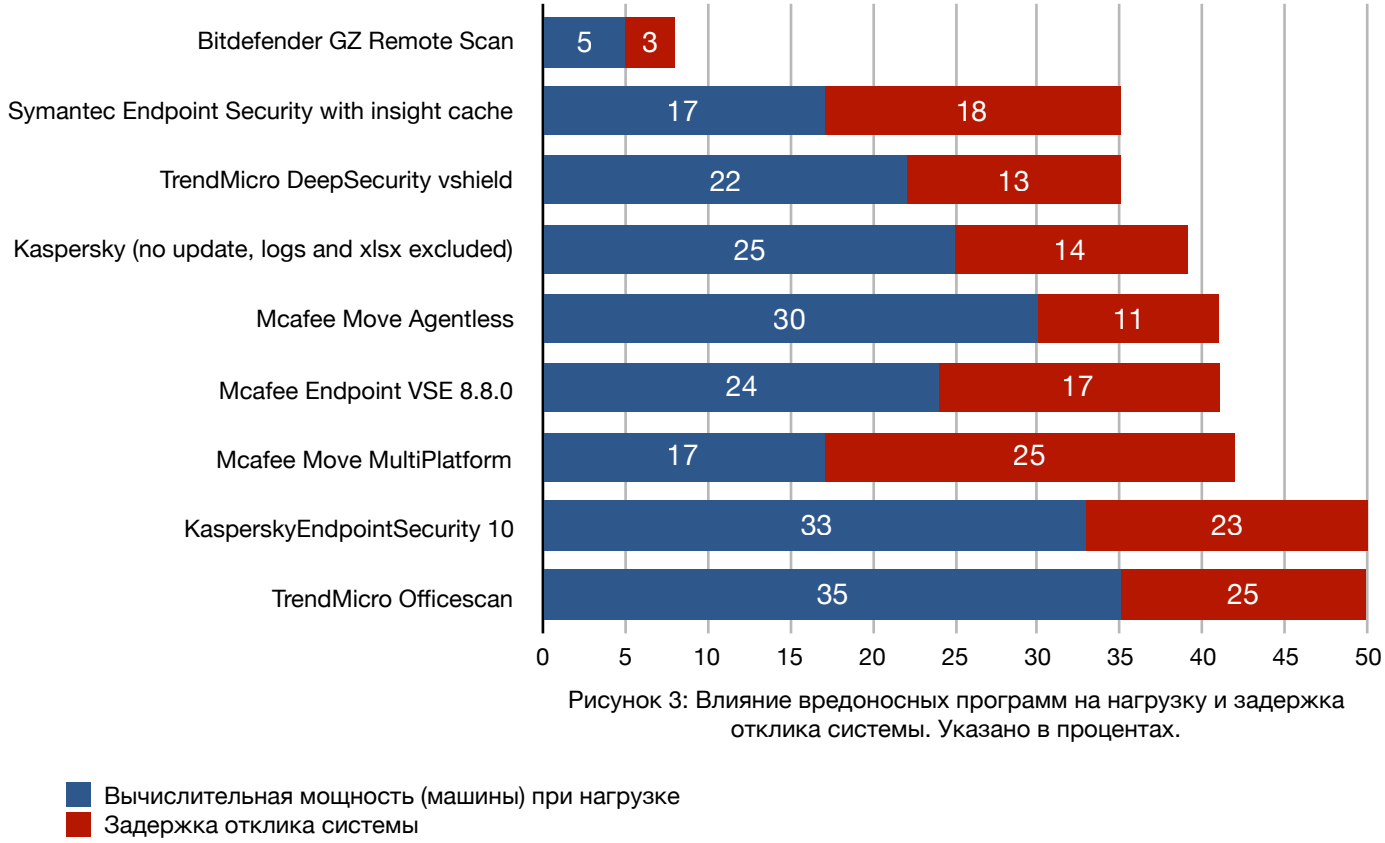

Рисунок 3: Влияние вредоносных программ на нагрузку и задержка отклика системы. Указано в процентах.

Поскольку общая картина зависит как от VSImax, так и о
т базового уровня, результаты были объединены на рисунке 3.
Задержка выражается в процентном увеличении базового уровня по сравнению с выполнением того же теста без установленного вредоносного ПО. Вычислительная мощность представляется как процентное увеличение нагрузки на аппаратное обеспечение, прикладываемое каждым экземпляром VDI, путем сравнения VSImax каждого решения с VSImax без установленного вредоносного ПО.

Заключение

Без сомнения безопасность имеет первостепенное значение для сохранения целостности данных. Однако безопасность никоим образом не должна препятствовать развитию бизнеса. Выбор правильного решения для обеспечения безопасности это разница между успешным проектом виртуализации и дополнительными капитальными затратами на большее количество оборудования, разочарованными сотрудниками и потерянной производительностью. В среде VDI внедренное решение по обеспечению безопасности должно оказывать минимально возможное влияние – более короткое время ожидания открытия приложений приводит к повышению производительности труда сотрудников и, следовательно, к меньшему количеству обращений в службу поддержки.

GravityZone Security для виртуальных сред это всеобъемлющее решение для обеспечения безопасности, специально разработанное для любой виртуализированной инфраструктуры. Когда SVE (Storage Virtualization Engine – виртуализация памяти, виртуализация системы хранения) развертывается в среде VDI, она поддерживает наибольшее количество сеансов VDI, достижимое по сравнению с любым другим решением для обеспечения безопасности виртуализации, доступным на рынке. Что также сводит к минимуму влияние задержки отклика, обеспечивая защиту от вредоносных программ в отношении файлов, памяти, процессов и реестра.

По сравнению с другими решениями по безопасности виртуализации, использование SVE в среде VDI дает:

- Более эффективную экономию средств.
- Более короткое время отклика приложения.
- Увеличение количества сеансов VDI.
- Гибкость использования любого гипервизора.
- Комплексная защита файлов, памяти, процессов и реестра.

Приложение

Методика тестирования

Все решения по безопасности были установлены и протестированы с минимальной стандартной конфигурацией, с активированными по умолчанию антивирусными и функциями против вредоносного ПО.

VSImax v4 (Макс. число VDI): VSImax v4 показывает количество одновременных сеансов, которые могут быть запущены в системе до ее насыщения. Это число указывает на масштабируемость среды (чем выше, тем лучше).

VSIbase: VSIbase указывает на производительность системы при отсутствии нагрузки на программную среду, оболочку. Эта величина используется для определения порога производительности. VSIbase дает представление о базовой производительности программного окружения (чем ниже, тем лучше).

Порог VSImax v4: Порог VSImax v4 указывает точку насыщения среды и основан на VSIbase. Пороговое значение для общего времени отклика составляет: средневзвешенное время отклика фазы базового уровня + 2600 мс.

Расчет VSImax v4. Моделируемая рабочая нагрузка на настольный компьютер записывается в виде 48-минутных циклов, в течение которых пользователь, моделируемый Login VSI, выполняет обычные действия в MS Office.

В каждом цикле время отклика двенадцати конкретных операций измеряется через регулярные интервалы.

Время отклика этих действий взвешивается до их добавления к общей сумме в %, чтобы гарантировать, что каждое действие оказывает одинаковое влияние на общее время отклика. Взвешивание используется следующим образом:

Действие – запуск:	Вес (%)
VSI Блокнота (Notepad) с большим текстовым файлом	50%
Диалогового окна открытия файла	125%
Диалогового окна начала печати	400%
Файла Zip PST (Outlook), файла без сжатия	600%
Файла Zip PST, файла с высокой степенью сжатия	17,5%
MS Word с новым документом	15%

1. VsiMax Dymanic (мс): Формула для динамического порога: Среднее время отклика базового уровня x 125% + 3000. В результате, когда время отклика базового уровня равно 1800, порог VSImax теперь будет 1800 x 125% + 3000 = 5250 мс.
2. VsiMax # VDI: когда ответ (мс) всех сеансов превышает VsiMax Dymanic (мс), достигается «Максимальное количество зарегистрированных (подключенных) сеансов» (VsiMax # VDI) «Конец теста»;
3. Количество машин: перед началом реальных тестов запускается несколько VDI, ожидающих, когда Login VSI подключит их к программной среде. 220 виртуальных машин запускаются в начале каждого теста. Это выполняется для лучшей имитации производственной среды, в которой может произойти сбой подключения. Поэтому число «VDI в режиме ожидания» больше, чем число «VDI, подключенных (login) к системе», и оно должно быть постоянным, чтобы сделать количество тестов VDI одинаковым для всех тестовых прогонов.
4. Период проведения тестирования. Средство тестирования Login VSI Tool запускает сеансы, между запущенными сеансами должна быть некоторая задержка. Это значение устанавливается перед тестированием для калибровки Login VSI для программного окружения. Значение «интервала времени» – это общее время, выделенное для запуска всех 220 сеансов. Инструмент тестирования Login VSI Tool

будет подключать (login) пользователей к системе каждые 16 секунд. Это означает, что он должен завершить подключение всех пользователей в течение 3600 секунд.

5. Высокие рабочие нагрузки. Большая рабочая нагрузка требует более высокой загрузки памяти и ЦП, поскольку все больше приложений выполняется в фоновом режиме. Такая рабочая нагрузка моделирует крупного пользователя (с большим числом машин). После начала сеанса большая нагрузка будет повторяться каждые 12 минут. Во время каждой операции время отклика измеряется каждые 2 минуты.

- Большая нагрузка при открытии до 8 приложений одновременно.
- Скорость печати составляет 130 мс на символ.
- 40 секунд простоя для имитации реальных пользователей.
- Каждый цикл после открытия будет использовать следующие программы:
- Outlook 2007/2010, просмотр 10 сообщений.
- Internet Explorer, одна вкладка оставлена открытой (BBC.co.uk), плюс открыты вкладки с браузерами для Wired.com, Lonelyplanet.com и тяжелым флеш приложением gettheglass.com.
- Word 2007/2010, один экземпляр для измерения времени отклика, один экземпляр для просмотра и редактирования документа.
- Виртуальный принтер Bullzip PDF Printer и Acrobat Reader, текстовый документ печатается и просматривается в PDF файле.
- Excel 2007/2010, открыт очень большой случайно выбранный лист.
- PowerPoint 2007/2010, просматривается и редактируется презентация.
- 7-zip: с использованием версии из командной строки, выходные данные сеанса архивируются.

6. Описание среды для тестирования:

- vCenter 5.5.0 1476327
- VMware Tools 9.4.0, сборка-1280544
- VDI Manager VMware View 5.0.0 сборка 481677
- vShield Manager Выпуск 5.5.3-217697
- Endpoint Driver Версия 5.5.0 1331820 (мультиплексор)

Базовая машина (хост) 1 (Dell R710) 5.5.0 1331820

- Процессор 2 x Xeon E5645 @2.4 ГГц
- Оперативная память 128 ГБт DDR3
- Контроллер внешней памяти Perc H700
- Жесткие диски 5 x OCZ Vertex 3 объединенные в массив с резервированием 0 Config
- Сетевая карта 2 x Gigabit Ethernet

Базовая машина (хост) 2 (Dell R710) 5.5.0 1331820

- Процессор 2 x Xeon E5645 @2.4 ГГц
- ОЗУ 128ГБт DDR3
- Контроллер внешней памяти Perc H700
- Жесткие диски 5 x OCZ Vertex 3 объединенные в массив с резервированием 0 Config
- Сетевая карта 2 x Gigabit Ethernet

Политика тестирования:

- Сканирование всех файлов
- Сканирование сетевых файлов
- Архивы, исключенные из сканирования
- Почтовые архивы, исключенные из сканирования
- Windows 7 X86 SP1, с обновлениями
- Программа дефрагментации был отключена
- Индексатор поиска отключен
- Обновление Windows отключено
- Запланированные задачи отключены
- Брандмауэр деактивирован
- Защитник Windows отключен
- Авто-обнаружение веб-прокси отключено
- Темы оформления отключены
- Superfetch (технология управления системной памятью) отключена
- Служба проверки совместимости приложений включена
- Автономные файлы отключены
- Центр обеспечения безопасности отключен
- Диспетчер отладки машины отключен
- Отчет об ошибках отключен
- 1172 ОЗУ выделено без резервирования
- 1 ядро виртуального процессора было выделено без резервирования
- Файл подкачки (Pagefile.sys) установить статическое значение 2x RAMv