Symantec Endpoint Protection в инфраструктурах VDI

Автор: Алексей Панкратов (ведущий эксперт, Symantec)
Дата: 06/11/2014

С развитием ИТ инфраструктуры организации нередко приходят к идее перевода физических рабочих станций в виртуальную среду VDI (Virtual Desktop Infrastructure), т.к. это позволяет более эффективно и гибко использовать имеющиеся ресурсы, а так же быстро реагировать на возникающие потребности.

При этом приходится решать ряд вопросов, на которые ранее обращалось мало внимания. Большинство из них связано с нагрузками, возникающими при одновременном выполнении действий на большом количестве виртуальных машин. Но есть и вопросы, связанные со способом создания и управления жизненным циклом машин.

Производители средств защиты учитывают специфику VDI-инфраструктур, при этом подходы порой разнятся. Далее мы расскажем, каким образом Symantec Endpoint Protection адаптирован для описанного сценария.

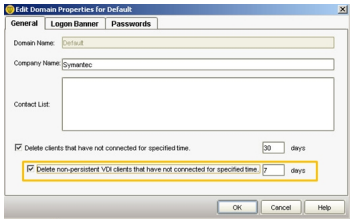
Высвобождение лицензий для non-persistent VDI клиентов.

Рассмотрим ситуацию, когда в организации есть как физические клиенты, так и VDI. Причем часть VDI клиентов являются непостоянными (non-persistent VDI), и могут удаляться через короткое время после создания. Без специальной оптимизации все лицензии будут довольно быстро использованы, т.к. лицензии удаленных VDI клиентов не высвобождены, а новые клиенты уже созданы.

Если клиент не имеет подключения к серверу в течение заданного времени (по умолчанию 30 дней), то Symantec Endpoint Protection может удалить его из списка клиентов и высвободить лицензию. Хотя этот параметр может меняться администратором, этого не всегда достаточно. Уменьшать значение периода удаления опасно, потому что физические клиенты или постоянные VDI клиенты могут находиться

в режиме offline вполне обоснованно: пользователь в отпуске, командировке и т.д.

Для разрешения затруднения нужно в non-persistent VDI (в мастер образ) добавить ключ реестра IsNPVDIClient и установить ему значение 1. После этого несложного действия Symantec Endpoint Protection Manager сможет выявлять клиентов non-persistent VDI и использовать отдельный параметр периода удаления:



Таким образом, можно избежать ситуации, когда лицензии окажутся задействованы уже удаленными non-persistent VDI клиентами.

AV Storm

В виртуальных средах существует риск возникновения такого явления как AV Storm. Опасность AV Storm заключается в том, что если все виртуальные клиенты одновременно начинают выполнять сканирование на вирусы, то подсистема хранения, процессор и память виртуального хоста испытывает заметное повышение нагрузки и потребления ресурсов, что, в свою очередь, может привести к деградации производительности системы и даже к остановке работы.

Во избежание реализации такого сценария Symantec Endpoint Protection имеет целый ряд технологий:

- Virtual Image Exception (VIE) - создание списка просканированных файлов в мастер образе для исключения их из последующих сканирований
- Shared Insight Cache (SIC) – исключение из сканирования файлов, уже

просканированных на других клиентах.

- Рандомизация времени начала сканирования – позволяет распределить в указанном временном промежутке момент начала сканирования.

Подробнее про технологии VIE и SIC мы уже рассказывали в предыдущей статье: http://www.vmgu.ru/articles/symantec-endpoint-protection-for-virtual-infrastructures
.

В сумме, использование этих инструментов позволяет заметно снизить нагрузку на дисковую подсистему, процессор и память, а так же сократить время сканирования. В ряде сценариев выигрыш может достигать 80%.

В случае именно non-persistent VDI клиентов, при правильной подготовке и поддержании в актуальном состоянии мастер-образа, рекомендуется вовсе отключать сканирование по расписанию. Файлы образа уже просканированы и добавлены в белый список, а новые и измененные файлы сканируются в реальном времени при обращении к ним (модуль защиты AutoProtect). Помимо этого рекомендуется включать функционал сканирования при входе в систему (allow startup scan to run when users log on).

Скачивание обновлений

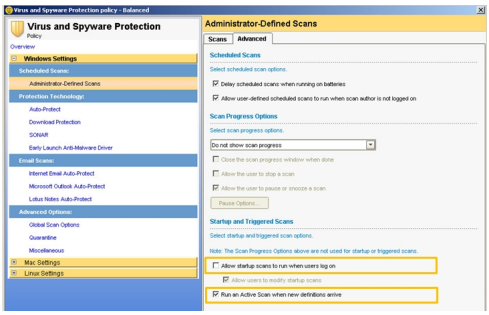
Помимо опасности возникновения AV Storm, в виртуальных средах возможен еще один сценарий, приводящий к повышению нагрузки на виртуальный хост (в особенности на дисковую подсистему): одновременный запуск скачивания обновлений антивирусных сигнатур и других модулей. Здесь Symantec Endpoint Protection также как и при сканирования задействует рандомизацию. Можно указать, на сколько часов момент начала сканирования может отличаться (как в плюс, так и в минус) от заданного времени.

К примеру, указав значение 4 часа, мы получим 8 часовой интервал времени, в котором будут запускаться задания на скачивание обновлений. Кроме того, следует помнить о мастер-образе, из которого разворачиваются VDI клиенты. Если этот образ устарел, то объемы скачиваемых данных будут больше. В связи с этим требуется регулярное обновление образа, а так же увеличение количества версий сигнатур, которые хранит

сервер управления.

Например, при максимальном «возрасте» мастер образа 2 недели, рекомендуется хранить сигнатуры за последние 30 дней. Если стоит задача снизить эпизодические (во время скачивания обновлений) нагрузки на сетевую инфраструктуру, то имеет смысл использовать механизм Bandwidth Throttling, который позволяет управлять количеством и скоростью соединений между клиентами и сервером управления.

Также следует обратить внимание на пункт настроек «Run an active scan when new definition arrive», который определяет нужно ли запускать сканирование сразу после скачивания обновлений. По умолчанию данная функция включена, но для виртуальных сред ее рекомендуется выключать.



В данной статье рассмотрены лишь некоторые моменты защиты виртуальных сред с помощью Symantec Endpoint Protection. В каждом конкретном случае нужно тщательно оценивать набор используемых средств и мер, что бы обеспечить максимальную защиту рабочей станции.

Более подробную информацию можно найти в статьях:

Read more http://feedproxy.google.com/~r/Vmguru-tech/~3/WKc5_me99OY/symantec-endpoint-protection-for-vdi