Kaspersky Security Center 10 SP3  
Kaspersky Endpoint Security 11

Пилотное тестирование

**Проверка режима Cloud AV**

В этом сценарии вы посмотрите, как новый режим работы KES11 c «легкими базами» влияет на количество потребляемой оперативной памяти.

Режим работы с «легкими базами» подразумевает, что будут скачиваться не все базы, а только самые необходимые, остальное будет проверяться по KSN. Использование «легких баз» позволяет существенно уменьшить размер дистрибутива KES и размер регулярных обновлений, а также уменьшить потребление ресурсов компьютера.

## Расскажите о себе

|  |  |
| --- | --- |
| Полное имя |  |
| Компания |  |
| E-mail |  |
| Телефон |  |

## Подготовьте:



* Сервер администрирования, на котором установлен Kaspersky Security Center 10 SP3
* Клиентский компьютер с Kaspersky Endpoint Security 11, который находится под управлением Kaspersky Security Center 10 SP3

|  |  |  |
| --- | --- | --- |
|  | Сервер администрирования | Клиентский компьютер |
| Операционная система |  |  |
| Версия Kaspersky Security Center |  |  |
| Версия Kaspersky Endpoint Security |  |  |

# Задание 1. Убедитесь, что режим работы с «легкими базами» включен по умолчанию

В Консоли KSC на Сервере администрирования

1. Откройте узел Policies
2. Откройте политику Kaspersky Endpoint Security 11
3. Перейдите в раздел Advanced Threat Protection | Kaspersky Security Network

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Опция Enable cloud mode for protection components включена |  |

1. Запустите задачу Download updates to repository на Сервере администрирования и дождитесь ее завершения
2. Обновите базы на клиентском компьютере с помощью групповой задачи обновления баз

На клиентском компьютере

1. Откройте диспетчер задач: нажмите сочетание клавиш WIN+R и введите команду taskmgr
2. Обратите внимание сколько памяти занимает процесс avp.exe, который запущен под учетной записью SYSTEM

Смотрите значение в колонке Commit Size; по умолчанию эта колонка не отображается, поэтому включите ее в свойствах диспетчера задач

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Commit size у системного процесса avp.exe составляет около 250 МБ | [Укажите свой объем] |

1. Не закрывайте диспетчер задач

# Задание 2. Переключитесь в режим работы с полными базами

В Консоли KSC на Сервере администрирования

1. Откройте политику Kaspersky Endpoint Security 11
2. Перейдите в раздел Advanced Threat Protection | Kaspersky Security Network
3. Выключите опцию Enable cloud mode for protection components

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Опция Enable cloud mode for protection components выключена |  |

1. Обновите повторно базы на клиентском компьютере с помощью групповой задачи обновления баз

На клиентском компьютере

1. Перейдите в окно диспетчера задач

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Commit size у системного процесса avp.exe составляет около 280 МБ | [Укажите свой объем] |

# Задание 3. Проверьте как режим Cloud AV Mode влияет на статус компьютера

В Консоли KSC на Сервере администрирования

1. Откройте политику Kaspersky Endpoint Security 11
2. Перейдите в раздел Advanced Threat Protection | Kaspersky Security Network
3. Включите опцию Enable cloud mode for protection components
4. Выключите опцию Use KSN Proxy

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Опция Enable cloud mode for protection components включена; опция Use KSN proxy выключена |  |

На клиентском компьютере

1. Cделайте так, чтобы клиентский компьютер не имел доступа в интернет, но имел доступ к Kaspersky Security Center.
2. Установите неверные настройки прокси-сервера, измените путь к Default Gateway или заблокируйте пакеты на gateway-сервере.
3. В результате доступ к KSN серверам должен быть заблокирован.

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
| Клиентский компьютер не имеет выход в интернет, но может общаться с Kaspersky Security Center |  |
|  |  |

В Консоли KSC на Сервере администрирования

1. Перейдите в узел Managed devices на закладку Devices
2. Подождите некоторое время, может занять 10-15 минут
3. Откройте свойства клиентского компьютера и перейдите в раздел Protection

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Статус клиентского компьютера Critical и описание статуса KSN servers unavailable |  |

На клиентском компьютере

1. Восстановите подключение к Интернет (откройте свойства сетевого подключения и восстановите адрес шлюза для протокола IPv4)

В Консоли KSC на Сервере администрирования

1. Подождите некоторое время, может занять 10-15 минут

|  |  |
| --- | --- |
| Ожидаемый результат | Наблюдаемый результат |
|  |  |
| Статус клиентского компьютера OK/Visible in network |  |

### Комментарии

|  |
| --- |
|  |