Настраиваем Microsoft WSUS для обновлений по SSL

Дано:

- Домен Active Directory
- Сервер Certification authority (CA) в данном домене (ca.mydomain.int)
- Сервер WSUS на базе Windows Server 2008R2, работающий без SSL на порту 8530 (wsus.mydomain.int)

Надо:

- Перевести раздачу обновлений на протокол SSL (патамушта Microsoft пишет: «the best practice»)

Создание сертификата и импорт его в IIS

На сервере IIS, обслуживающем WSUS делаем следующее:

- Запускаем «Диспетчер служб IIS»
- Щелкаем на WSUS, открываем «Сертификаты сервера»
- В Действиях выбираем «Создать запрос сертификата», заполняем поля, Далее, все оставляем по умолчанию, Далее, сохраняем запрос в файл WSUS-request.txt
- Открываем Блокнотом файл WSUS-request.txt
- Запускаем любимый браузер, переходим на сервер сертификации http://ca.mydomain.int/certsrv/
- Щелкаем «Запрос сертификата» → «Расширенный запрос сертификата», в поле «Сохраненный запрос» вставляем содержимое файла WSUS-request.txt, «Шаблон сертификата» меняем на «Веб-сервер», нажимаем «Выдать», на новом экране нажимаем «Сохранить сертификат» и сохраняем где-нибудь с понятным именем, например WSUS-Answer.cer
- Переходим обратно в «Диспетчер служб IIS», в Действиях выбираем «Запрос установки сертификатов», выбираем наш получившийся файл WSUS-Answer.cer, в поле «Понятное имя» пишем имя сертификата, например «WSUS-certificate», переключатель «Выбрать хранилище сертификатов для нового сертификата» выбираем «Размещение веб-служб», нажимаем OK.
- Если получаем ошибку HRESULT: 0x80070005 (E_ACCESSDENIED) - значит не хватает прав, делаем следующее:
  - Открываем свойства папки C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys и даем на нее полные права для «Администраторы» и «Все»

Настройка сайта "Администрирование IIS"

- В «Диспетчер служб IIS» выбираем наш сайт «Администрирование IIS», в Действиях выбираем «Привязки»
- Если порта HTTPS с номером 8531 нет - создаем его, если есть - редактируем

- Заполняем поля:
  - IP-адрес: «Все неназначенные»
  - Порт: 8531
  - Имя узла: wsus.mydomain.int (но можно и не указывать)
  - SSL-сертификат: выбираем наш добавленный сертификат «WSUS-certificate»
  - Нажимаем «Вид», смотрим наш сертификат, убеждаемся что он валидный и действительны все сертификаты в пути сертификации
  - OK, Закрыть
  - Теперь защитим подключения к нашим службам, для этого для папок ApiRemoting30, ClientWebServices, DssAuthWebService, ServerSyncWebService, SimpleAuthWebService делаем следующее:
    - выбираем папку щелчком на ней
    - открываем «Параметры SSL»
    - Ставим галочку «Требовать SSL», «Сертификаты клиента» должны быть «Игнорировать»
    - Нажимаем в Действия «Применить»

Распространяем сертификат WSUS при помощи Групповых Политик

На контроллере домена открываем редактор групповых политик, создаем новую политику (или добавляем в уже существующую), переходим в раздел Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политики открытого ключа → Доверенные корневые центры сертификации и добавляем корневой сертификат нашего домена и сертификат WSUS-сервера (тот самый WSUS-Answer.cer)

Связываем эту политику с OU или доменом - как удобнее.

Настраиваем обновление WSUS через Групповые Политики

Редактируем раздел Конфигурация компьютера → Политики → Административные шаблоны → Компоненты Windows → Центр обновления Windows → Указать размещение службы обновлений Microsoft в интрасети

В самом просто и распространенном случае оба параметра будут равны «https://wsus.mydomain.int:8531/»

Обновляем клиентские компьютеры

Пока на клиентских компьютерах не загрузились сертификаты и не обновились настройки WSUS - они будут показывать разлиыне кодовые ошибки.

Для принудительной синхронизации запускаем как обычно

```
> gpupdate /force
```

и запускаем WSUS проверить обновления:

```
> wuauclt /detectnow
```

Если все хорошо и есть обновления для установки - они начнут загружаться, иначе «Windows не требуется обновление».

microsoft, wsus, iis, ssl, 8531, 0x80070005, E ACCESSDENIED